1-1-1997

Transforming the paradigm for crafting acceptable use policy : managing the electronic commons.

Robert A. Reilly
University of Massachusetts Amherst

TRANSFORMING THE PARADIGM FOR CRAFTING ACCEPTABLE USE POLICY: MANAGING THE ELECTRONIC COMMONS

A Dissertation Presented

by

ROBERT A. REILLY

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF EDUCATION

February 1997

Education

TRANSFORMING THE PARADIGM FOR CRAFTING ACCEPTABLE USE POLICY: MANAGING THE ELECTRONIC COMMONS

A Dissertation Presented

by

ROBERT A. REILLY

Approved as to style and content by:

G. Ernest Anderson, *Chair*

Margaret McDevitt, *Member*

Douglas E. Abbott, *Member*

M. Ethan Katsh, *Consultant*

Bailey W. Jackson, *Dean*
School of Education

DEDICATION

This dissertation is dedicated to three people—my wife, Mary Reilly, and my parents, Bernadette and Martin Reilly.

Mary has sustained me through the trials and tribulations of the doctoral process. She has shouldered virtually all the household duties that I would normally be expected to do. Without her support I would not have been able to even consider entering, let alone, be completing the doctoral process. Much of my doctoral degree belongs to my wife—my best friend—Mary.

I also must make note of the support of my parents—Martin and Bernadette. They have been supportive of all my endeavors from my enlisting in the Army during the Vietnam War, to my Bachelor's degree at UMass in Amherst, to my Master's degree at Springfield College, and now through this doctoral process. Through all this they have done what good parents do—they quietly support the things their children do.

EPIGRAPH

[T]he Net isn't just another communications medium . . . the Net is a place that encompasses almost every communicative aspect of daily life now, and that will be increasingly central to all American lives . . . [The courts can no longer] tell themselves that when they uphold governmental content regulation in that medium, American public life and Americans' access to information in general won't suffer much. Lots of folks believe that one reason broadcasting regulation is tolerable is that, on balance, the public doesn't lose much of its overall access to information under that regulation. You can still read books and newspapers . . . [The] Net is about something more than access to information, and . . . putting the Net under federal content-control rules makes no more sense than putting conversations on the street, or in parks, or in meeting halls under those same rules. . . [It is necessary to steer the courts away from] any "balancing" between the *particular* rights *of some kinds* of publishers and the need to address a perceived social harm. Instead, they needed to see the case as the weighing of a whole range of communications that take place daily in American public and private life against the need, if any, to put the whole thing under federal control to remedy the perceived harm.

Michael Godwin. (1996, June 15). Posted to the Virtual Communities Conference on the WELL (Whole Earth Lectronic Link), San Francisco, CA.

ACKNOWLEDGMENTS

As I have come to understand, the doctoral process is not an individual effort. Where it may at first appear so, such is not the case. A person cannot navigate the doctoral process without a large supporting cast of people who believe in you and what he is doing. I have been very fortunate in being able to call upon a very distinguished supporting cast.

The most important person in this process has been my mentor, friend, and advisor since the days before I began the doctoral process—Professor G. Ernest Anderson. As the chairman of my doctoral committee, Dr. Anderson has been many things to me: a silent but *watchful observer*, a *gentle guiding hand*, and when the need has arisen, has been a *forceful motivator*.

Associate Vice Chancellor for Information Technologies and Professor of Mechanical Engineering Douglas Abbott has been a member of this doctoral committee since it was formed. Dr. Abbott has given of his time to be a key advisor to me. As the senior administrator for technology on the Amherst campus, he could have easily declined to advise a doctoral student. The demands of his position leave little time for academic advising. Dr. Abbott has been a patient supporter of a *not ready for prime time* doctoral student. With his guidance and support, experiences that would not have been possible for the typical doctoral student became commonplace. His wisdom and guidance will always be remembered and greatly appreciated.

I would be remiss without mentioning the assistance given to me by Dr. Marcellette Williams, Deputy Chancellor. She has provided me with first hand experience in the development of university system-wide computer use policy by appointing me to the University's Information Technology Policy sub-committee.

I deeply regret that I cannot thank Professor Byrd Jones for his invaluable support and guidance as this doctoral process draws to a close. Dr. Jones's untimely death shortly after the comprehensive examination was a great loss to my committee, and to me personally. His counsel and wit will be greatly missed. Dr. Jones had a very full schedule of classes and a number of advisees—and still found time for me. His willingness to devote time and space in his busy day to, yet another doctoral student reflects the care and concern.

This dissertation and the completion of the doctoral process would not have been possible without the support and guidance of Professor M. Ethan Katsh of the Legal Studies department. He has given of his time and expertise through this entire doctoral process. His unhesitant willingness to advise a doctoral outside of his department and above and beyond any university obligation is highly commendable and worthy of note. His enthusiastic support of scholarship merely for the sake of scholarship is an example worthy of long admiration and emulation.

Dr. Margaret McDevitt, Dean of Academic Resources and Technology at Middlesex Community College in Bedford very graciously became a member of the doctoral committee due to the death of Dr. Byrd Jones. She has assumed the responsibilities of a committee member in a very expeditious and professional manner.

time from his position in the Keene, New Hampshire, school system to provide guidance to a doctoral student in need of his support and expertise.

I have received and benefited from expertise and assistance of professors and scholars whom I have not, as yet, physically met. In this regard I owe a great debt to four law school professors and one attorney who have selflessly given of their time to comment upon my dissertation proposal and the dissertation itself. Words cannot express the gratitude that is in order for: Daniel Burk, Professor of Law, Seton Hall University; Michael Froomkin, Professor of Law, University of Miami; Trotter Hardy, Professor of Law, William and Mary University; Mark Lemley, Professor of Law, University of Texas at Austin; and Lee Tien, Attorney at Law, Berkeley, California.

Last, but certainly not least, the concessions that my employers have allowed for my doctoral study cannot be overlooked. Mr. Alan Genovese, Superintendent of Schools, and Mr. Thomas Gillooly, Principal of Lanesborough School, have been supportive and understanding of the demands of a full-time doctoral program. Needless to say, without their ascent and continued support, I could never have started, let alone finished this doctoral program.

ABSTRACT

TRANSFORMING THE PARADIGM FOR CRAFTING ACCEPTABLE USE POLICY: MANAGING THE ELECTRONIC COMMONS

FEBRUARY 1997

ROBERT A. REILLY, B.S., UNIVERSITY OF MASSACHUSETTS AMHERST

M.Ed., SPRINGFIELD COLLEGE

Ed.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by Professor G. Ernest Anderson

There is a need to solidify the common folklore understanding of what acceptable behaviors are for computer network users. The process of solidification should provide for the development of a paradigm that will be utilized in the formulation of computer use policy. Those who craft computer use policy should move away from the model of a *network as a superhighway* to a model of a *network as a commonly shared resource*.

The current process for formulating and reviewing an Acceptable Use Policy—an AUP—has generally not evolved as quickly as the rapidly expanding user base and changing demographics. Given the changes in user demographics on computer networks, there is a rapidly growing need to better understand the computer network and to create AUP's based upon questions of social interaction.

Such questions might attempt to address the issues of cooperation and sharing of resources. For example, faced with the temptation to behave selfishly—to overuse the resources, how can a group of people (through its AUP) establish and maintain cooperative behavior?

To begin the process of answering such questions, this dissertation suggests focusing on the question: "How do privacy aspects of the First and Fourth Amendments impact the formulation of Acceptable Use Policy for an on-line computer network?" This dissertation suggests that privacy is a foundational concept in developing an understanding of the nature of the social activities which are growing in cyberspace. This dissertation also chronicles the transition from informal *gentleman's agreement* AUP's toward more formalized ones.

The research in this dissertation was accomplished by accessing a number of legal resources such as Lexis/Nexis, Westlaw, Web sites on the Internet, a law library, and several Mailing Lists involved in discussions of online legal issues. Other sources, such as government documents, existing and out of date Acceptable Use Policies, and legislative testimony, were reviewed. Personal communication with a number of eminent legal scholars also provided a valuable resource.

This dissertation concludes that an Acceptable Use Policy should be in place to govern use of computer networks. The Acceptable Use Policy should become much more of a social contract in the manner of many campus faculty and student handbooks, and, even in the manner that the U.S. Constitution is a social contract for

the U.S. population. AUP's should be locally developed by those who have a foundational understanding of:

- legal principles of privacy, search and seizure, and due process, and,
- management theory involving the use of commonly shared resources.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABA	American Bar Association
ACLU	American Civil Liberties Union
AUP	Acceptable Use Policy
CAUSE	College and University System Evaluation
CDA	Communications Decency Act
CPSR	Computer Professionals for Social Responsibility
ECPA	Electronic Communications Privacy Act
EFF	Electronic Frontier Foundation
EPIC	Electronic Privacy Information Center
ERIC	Educational Resources Information Center
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FOIA	Freedom of Information Act
IETF	Internet Engineering Task Force
NCIC	National Crime Information Center
NII	National Information Infrastructure
NSA	National Security Agency
NSFNET	National Science Foundation's Network

INTRODUCTION

Author's Note: A number of citations contained in this dissertation refer to legal material. Legal citations vary somewhat, in form, from the traditional APA references. Legal materials are cited in conformance with the APA Publication Manual's (p. 223) requirement to utilize the conventions in the Bluebook: A Uniform System of Citation (1991).

Historically, Acceptable Use Policy (AUP) primarily regulates user-to-computer behavior with the use of the Internet. There has been a radical change and a demographic shift in both the nature of the network and its uses. The Net is fast becoming a mirror of the real world community. The Net is becoming a community rather than an information resource or an information superhighway. Those who craft policy should adjust their paradigm for formulating policy—a paradigm which seems to be based upon the network as a mechanical entity. The Net is a growing community and this dissertation suggests that the paradigm for AUP creation/revision should change to view the Net as a shared community resource. In order to reformulate the paradigm from its present situation to one which addresses the social and communal needs, those who craft AUP's should have a foundational understanding of the legal concepts of privacy, search and seizure, and due process. They should also have a working understanding of the principles and theories of managing and setting policy for commonly shared resources.

CHAPTER I

THE PROBLEM: THE POLICY CREATION PROCESS

> We are currently in a period of transition. More and more people are becoming aware that the computer is an extraordinary communicative device, are learning how to send and receive information via their computers, and are gaining access to computer based telecommunication networks. As this transition continues, we will not only develop a new understanding of the novel and powerful modes of distributing information electronically, but we will also realize more clearly that this powerful new medium of communication has significant implications for law.[1]

Background of the Problem

> The press, the machine, the railway, the telegraph are premises whose thousand-year conclusion no one has yet dared to draw.[2]

There is a need to solidify the common folklore understanding of what acceptable behaviors are for computer network users. Public institutions[3] of higher education should begin to transition from an informal understanding of acceptable use to a more formal structure based upon a social-legal paradigm. The current process for formulating and reviewing an Acceptable Use Policy[4]—an AUP—has generally not evolved as quickly as the rapidly expanding user base and changing demographics (Figure 1). Prior to 1993, on-line computer systems were predominantly utilized by

---

[1] Ethan Katsh, Law in a Digital World, 38 Villanova L. Rev. 403, 407 (1993). See generally, Elizabeth Eisenstein, The printing press as an agent for change.

[2] Friedrich Nietzsche. (1880). The philosophy of Nietzsche. New York: Modern Library.

[3] This study focuses upon state institutions. For private institutions, the 'computer use policy' question can be solely a question of contract law. With regard to state institutions, the question may still boil down to a matter of contract law; but other issues still exist given public institutions are extensions of the government where private institutions are not.

[4] An Acceptable Use Policy (AUP) refers to a document which defines what the computer user's rights and responsibilities are to the system itself, other users, and to the administrators of that system. The AUP also defines what the administration's rights and responsibilities are to the system itself, and to the users of that system. AUP's also insure access to information and communication while ensuring that the resource use does not overburden the system's capabilities.

academics and researchers, who tended to be very like-minded as to network use and etiquette—they seem to have a common understanding of online ethics, customs, and rituals. More recently, on-line systems are being utilized by a highly diverse general public, and usage is generating a need for rules in a digital world that accurately reflect the real world. The once held 'common understanding of online ethics, customs, and rituals' is no longer a commonly held understanding.

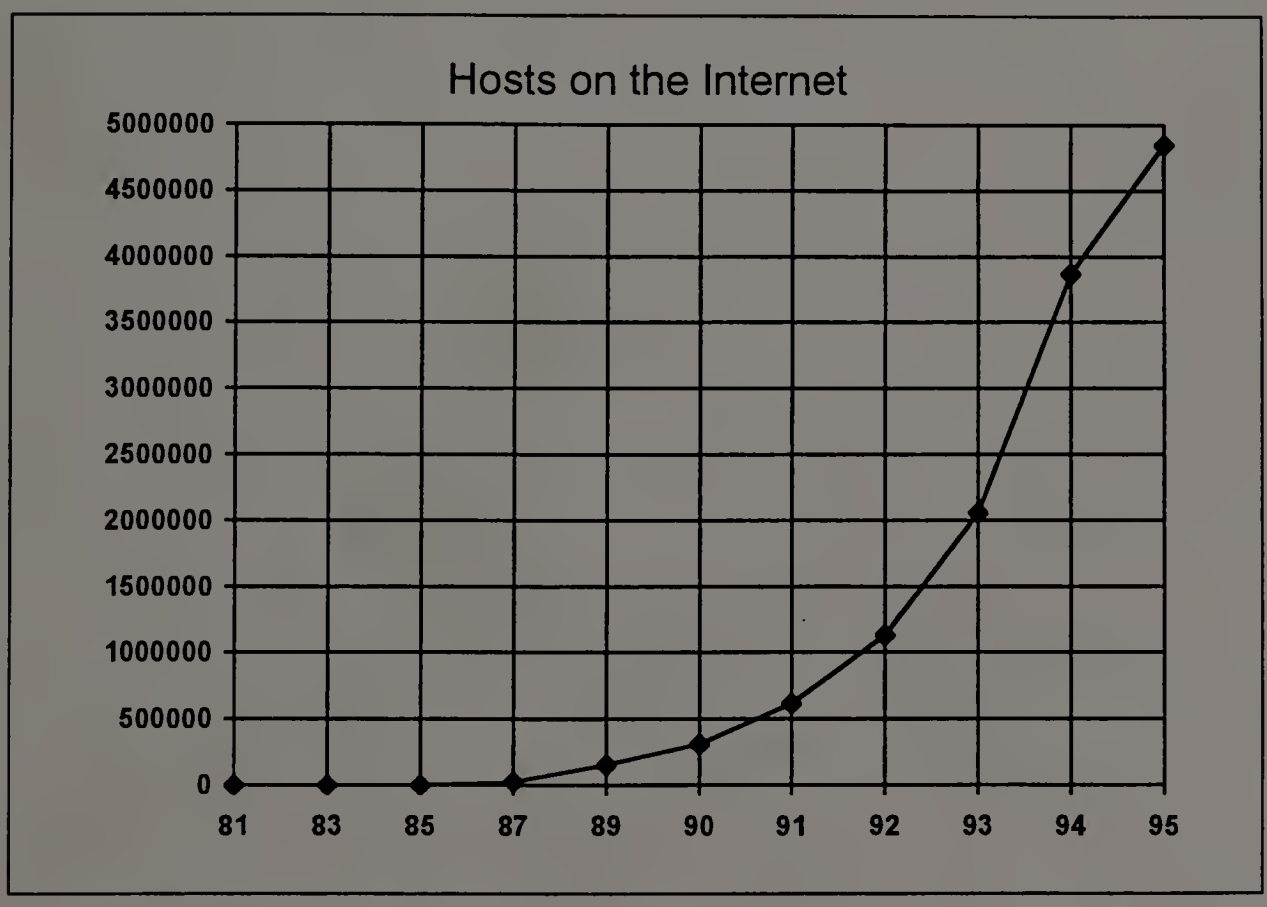

Figure 1 - Hosts on the Internet 1981-1995[5]

---

[5] This document is Available as of July 1, 1996: http://NIC.MERIT.EDU/nsfnet /statistics /history.hosts. Anthony Rutkowski, Executive Director of the Internet Society, states that "a commonly used method of estimating the total number of Internet users is to multiply the number of host computers by 10. For example, in 1993, [there were] about 20 million users." Id.; See also, John S. Quarterman. (1995, March 3). Internet communications services on NSFNET. Matrix News, 5(3) [On-line]. Available as of July 1, 1996: gopher: //akasha.tic.com:70/matrix /news /v5/ports.501.

The process of policy change has also not evolved[6] as quickly as has the capabilities of technology. In their 1890 law journal article, Warren and Brandeis advocated that new developments in technology and business methods require the next step be taken to expand the right of privacy to be a right "to be let alone."[7] It was not until 1967 when the Supreme Court[8] broadened the scope of privacy to recognize that, given the technology of the day, a physical intrusion or trespass into a given area was not the only way to invade a person's privacy. Today, as Fulton noted, "[t]echnological change often outpaces the law . . . [and that] [e]xamining the legal implications of emerging technologies can help narrow this gap."[9]

Currently, the process of crafting a university AUP is based upon a model of an on-line computer network as a *superhighway*. A *superhighway* metaphor may not be the best foundation from which to draw a model of social behavior. As Kollock and Smith note:

---

[6] Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994). See generally, Anne M. Fulton, Cyberspace and the Internet: Who Will Be The Privacy Police?, 3 Comm. Law Conspectus 63 (1995).

[7] Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harvard L. Rev. 193 (1890).

[8] Katz v. United States, 389 U.S. 347 (1967). Defendant Katz was, convicted in the United States District Court for the Southern District of California, of a violation of statute proscribing interstate transmission of wire communication of bets or wagers, and he appealed. The Court of Appeals, 369 F.2d 130, affirmed, and certiorari was granted. The Supreme Court held that government's activities in electronically listening to and recording the defendant Katz's words spoken into telephone receiver in public telephone booth violated the privacy upon which the defendant justifiably relied while using the telephone booth. Thus this action constituted a "search and seizure" within Fourth Amendment, and the fact that electronic device employed to achieve that end did not happen to penetrate the wall of the booth could have no constitutional significance. The Court further held that the search and seizure, without prior judicial sanction and attendant safeguards, did not comply with constitutional standards. Although, accepting the account of the government's actions as accurate, the magistrate could constitutionally have authorized with appropriate safeguards the very limited search and seizure.

[9] Anne M. Fulton, Cyberspace and the Internet: Who Will Be The Privacy Police?, 3 Comm. Law Conspectus 63 (1995); See also, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994).

> with earlier technologies [which] promised freedom and power, the central problems of social relationships remain, although in new and possibly more challenging forms ... One of the most basic questions in the social sciences is the problem of cooperation. In the face of temptations to behave selfishly, how might a group of people ever manage to establish or maintain cooperative relations? The character and qualities of this problem are different when groups use [online computer systems].[10]

The IETF's (Internet Engineering Task Forces) AUP philosophy statement suggests a non-social model as the basis by which to craft AUP's. It states that AUP's are primarily used "to determine pricing, customer base, type and quality of service metrics, and a host of other provider services."[11] The IETF notes that the primary considerations are technical in nature when they state that:

> "[i]n defining your particular AUP there are three areas that must be addressed. They are where you get service from, who your peers are, and whom you provide service to. A good understanding of these concepts will make or break the AUP you formulate.[12]

The IETF's statement does note the need that future Acceptable Use Policies have a "better understanding of an AUP, [as] how to formulate one seems to be [an] increasingly important [need] as the global net encompasses new environments."[13] But this statement appears to be an after-thought on the part of the committee and does not appear to be a reflection of the position of the IETF AUP working group.

There is a significant quantitative change in the number of users on the Internet and on campus networks (Figure 1). There is also increased functionality on the Net (e.g., growth of the World Wide Web to support political campaigns,

---

[10] Peter Kollock and Marc Smith. (1994). Managing virtual communities: Cooperation and conflict in computer communities [On-line]. Available as of November 1, 1996: http://www.sscnet.ucla.edu/soc/csoc/vcommons.htm.

[11] AUP-Working Group of Internet Engineering Task Force. (1995, July). Acceptable use policy definition [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

[12] AUP-Working Group of Internet Engineering Task Force.

[13] AUP-Working Group of Internet Engineering Task Force.

business, the entertainment industry). This two-fold change (more functionality of the network, and more users) appears to be occurring both on the Internet at large and on campus networks. To be more specific:

- there are more varied users coming on line

Given the increasing diversity of available services and an increasing number of users, there is a greater concern about conducting the business of the computer network in a fair and equitable manner. Administrators should now be knowledgeable in regard to basic legal issues (e.g., invasion of privacy, search and seizure, eavesdropping, copyright infringement, harassment) as these issues will become a part of the conceptual reform in regard to the construction of an AUP.

- there is more socially diverse and anti-social behavior

Where once the Internet was a group of like-minded scientists, educators and researchers, it is fast becoming a mirror image of society in general. This diverse population is being confronted with behavioral norms more familiar in a research lab or an academic classroom. What was fair, equitable and universally accepted on the Net some years ago, is not fair, or equitable, or universally accepted now.

- there is a fuzzy legal area

Currently the AUP in general is crafted such that typical users can not understand its mandates. Present AUP statements tend to assume that the user has a fairly sophisticated understanding of computers and network etiquette. AUP statements should go beyond 'Ten Commandment' brevity.

- there are simply more people on the Net and on campus networks

There is a flood of people on campus networks (figure 2) . The mere presence of this many people necessitates that rules, customs, and metaphors be formalized.[14]

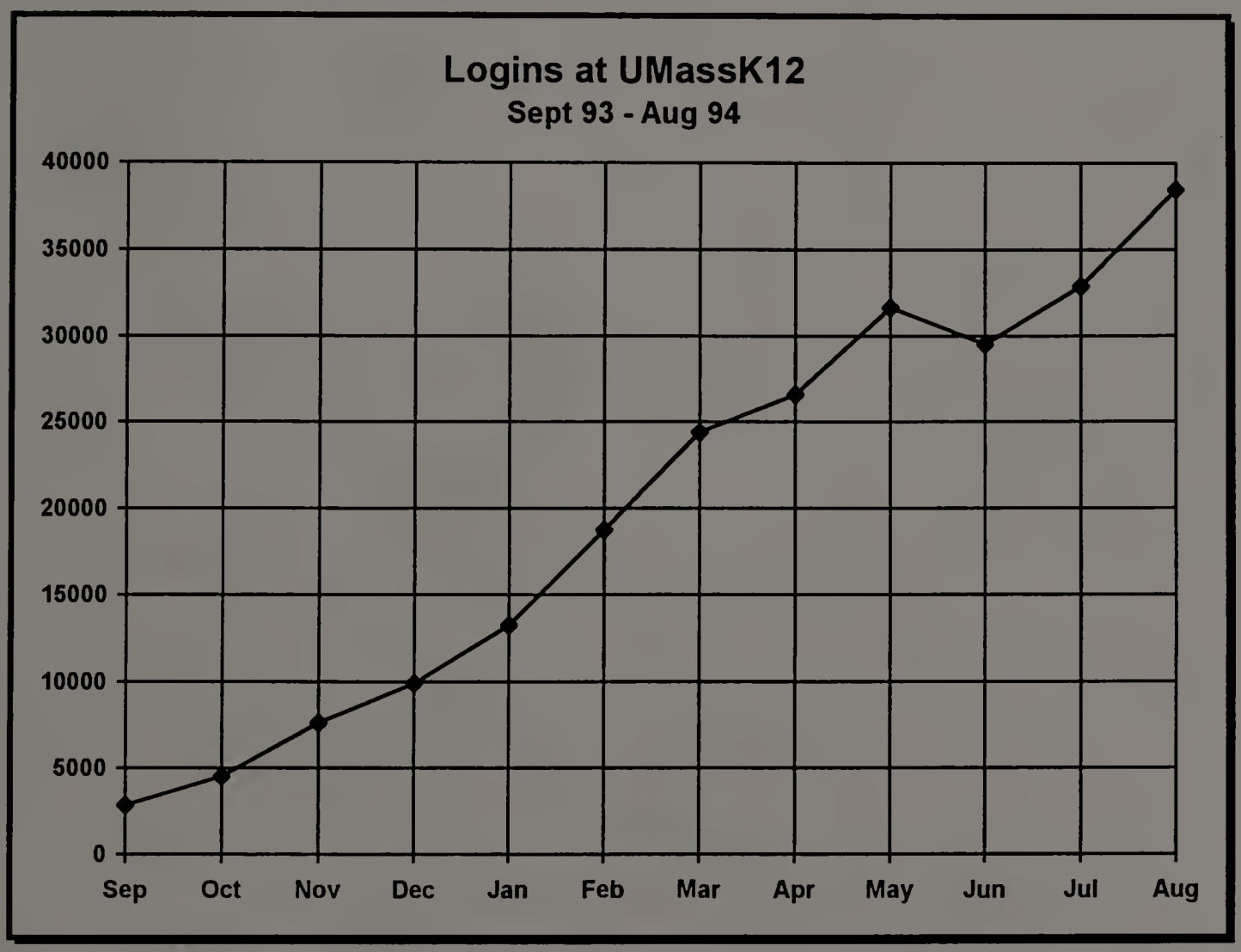

Figure 2 - UMassK12 Usage - September 1993 through August 1994[15]

[14] Bruce Sterling. (1995). The hacker crackdown. New York: Bantam Books, page 247.
[15] Data available as of July 1, 1996: ftp://k12.oit.umass.edu/statistics

Computer networks are rapidly becoming a mirror environment of the real world. Many of the things that one can do in the real world are now possible in the electronic world. But given the differences between the real and electronic world a number of real world laws lose their clarity and begin to warp when attempts are made to map them onto the electronic world.

Toward a Solution and Reform

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the demands of society.[16]

University administrators should address a number of issues when computer networks are utilized by members of the university community. The university is faced with a need to create, codify, and enforce policy for a vaguely defined environment. This vague definition is due to the multiplicity of means which can be employed in regulating a wide variety of dissimilar services which all occur within the same medium—cyberspace. Intellectual property rights, legal liability, security, user privacy rights, matters of search and seizure, and accuracy of information, to name a few, are all important aspects of computer network use which should be addressed in the Acceptable Use Policy.

The administrators of public institutions should have a doctrinal understanding of the issues (e.g., Constitutional level issues—privacy, search and seizure, due process) inherent in AUP development. Other overarching questions which will

---

[16] Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

impact on-line computer networks, but which will not be addressed in this study are: "What types of information and conversations can be suppressed? How can a university suppress inappropriate information—by restricting gathering, restricting distribution in general, restricting potential recipients, or restricting use? Who should have the right and who the duty to enforce the restrictions?"[17]

Acceptable Use Policies need to address such questions as:

- Are technologically illiterate users adequately informed of their responsibilities and rights on a computer network?,
- How are computing resources allocated?,
- How do the logistical/resource needs impact user's rights?,
- What are user's rights and responsibilities?,
- Who is entitled to use the system?,
- What actual legal authority is vested in a system administrator?

Given the demographic changes of users on computer networks, it is also important to investigate such questions as: can AUP statements facilitate community building, and thereby foster an understanding of social values and ethics on the network (of course, in addition to protecting the physical integrity of the computer network)? What will Acceptable Use Policy statements be in like in the future? What human behaviors should and can an AUP regulate? Can instilling privacy issues into an AUP facilitate a change in the AUP's nature from a focus on the operational and

---

[17] Peter B. Maggs, John T. Soma and James A. Sprowl. (1992). Computer law, cases, comments, questions. St. Paul, MN: West Publishing, page 490.

mechanical nature of the network to a focus on the community of users which populate the campus's network and/or their societal needs?

AUPs for public institutions can no longer be based upon the assumption that on-line computer systems are utilized exclusively for research and other academic purposes. More recently, on-line systems are being utilized by a diverse campus community which is generating a need for rules that reflect real world interactions occurring on the networks. The Internet Engineering Task Force (IETF) has cited a number of issues which need to be considered during framing of an Acceptable Use Policy. These issues include (but not limited to): "privacy, morals and ethics, freedom of expression, legal constraints, safety, harassment, plagiarism, resource utilization, indemnification, target areas of interest, and remedies and recourse."[18]

There are a number of other broad, inclusive issues that should also be considered. These issues address the very nature of a computer network. For example, "[l]iability for illegal activities in cyberspace is affected by how the particular computer information service is viewed."[19] If a computer system allows one entity to deliver messages to a large number of users, then the system may be viewed as a *publisher*. Many publishers are utilizing computer networks to supplement or publish editions of their product.[20] Some scholars are already referring to computer

---

[18] AUP-Working Group of Internet Engineering Task Force.

[19] David J. Loundy, E-Law: Legal Issues Affecting Computer Information Systems and System Operator Liability, 3 Alb. L.J. Sci. & Tech. 88 (1993).

[20] See Generally, T.L. Johnson. (1990, April 10). Fred the computer: Electronic newspaper services seen as *ad-ons*. Comm. Daily, 4.

networks as "the printing press of the 21st Century."[21] But Loundy argues that computer network "service are more like common carriers [(e.g., the telephone company)] than publishers."[22] The nature of computer systems will vary greatly depending upon the ultimate legal definition of on-line computer networks.

Each of these issues is of major importance to university administrators and could be the subject of a separate doctoral dissertation. Each is complex and not yet clearly defined by the law or by legal scholars. This study leaves these, and many other issues for other researchers to address. This dissertation will focus upon conceptual issues inherent in the formulation of an AUP as those issues pertain to a computer user's *right to privacy.*[23] This dissertation will also suggest that a paradigm shift is in order for those who craft an Acceptable Use Policy.

As computer networks become "the media through which more and more public discourse takes place, the ways in which that discourse is socially organized

---

[21] Ithiel de Sola Pool, quoted in John Markoff. (1990, May 13). Some computer conversation is changing human contact. NY Times, page 1.

[22] David J. Loundy, E-Law: Legal Issues Affecting Computer Information Systems and System Operator Liability, 3 Alb. L. J. Sci. & Tech. 79, 88 (1993).

[23] The *Right of Privacy* is a general right to be left alone. Katz v. United States, 389 U.S. 347 (1967). The *Right of Privacy* is a "generic term encompassing various rights recognized . . . to be 'inherent in the concept of ordered liberty' ... including protection from governmental indifference." Industrial Foundation of the South v. Texas Industrial Accident Board, 540 S.W.2d 668, 679 (1976). The four forms of invasion of privacy are unreasonable intrusion upon seclusion, appropriation of name or likeness, unreasonable publicity given to a person's private life, and placing another in false light before the public." 77 C.J.S. Right to Privacy and Publicity 488. Although the term *privacy* is not mentioned in the US Constitution, it has been defined by the Supreme Court, through the years, in a line of decisions. The Court has held in Griswold v. Connecticut, 381 U.S. 479 (1965) that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create 'zones of privacy'. The right of association contained in the penumbra of the First Amendment is one..."); See also, Roe v. Wade, 410 U.S. 113 (1972) (The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, ... the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution.)

becomes more consequential."[24] Given this concept, this dissertation also suggests that in order to reformulate the paradigm by which AUP's are created it may be necessary to address the issues of social interaction and social behavior on the network—the AUP would become a social contract[25] similar to the staff handbook and the student handbook. This dissertation suggests that a new paradigm for formulating an AUP should be based upon the concept of Hardin's "tragedy of the commons."[26] Hardin described a group of herders having open access to a common parcel of land—known as the *Common*—on which they could let their cows graze. It is in each herders interest to put as many cows as possible onto the land, even if the commons is damaged as a result. The herder receives all the benefits from the additional cows and the damage to the commons is shared by the entire group. Yet if all herders make this individually reasonable decision the commons is destroyed and all will suffer.

Hardin's model when coupled with a foundational understanding of the legal concepts of privacy, due process, and search and seizure appears to be a very powerful model by which to create a paradigm to craft Acceptable Use Policies in public higher education.

---

[24] Kollock and Smith.

[25] Right to privacy in the age of telecommunication [On-line] states that a "social contract reflects the agreement between the people and the government on how much power the people consent for the government to have and exert. The social contract between the people and the government exists so long as the government uses its powers within the due process of law and the people agree to the outcome of the due process of law. With the due process of law as a vehicle for maintaining the social contract, the government uses its power without compromising certain *natural and inalienable* rights of the individuals in a way unspecified by the Constitution, our social contract."

[26] Garrett Hardin. (1968). The tragedy of the commons. Science (162), page 1243-1248. Garrett Hardin. (1977). Managing the commons. San Francisco: W.H. Freedman and Co.

CHAPTER II

A REVIEW OF THE LITERATURE: COMPUTER NETWORKS, THE CONSTITUTION, USER PRIVACY AND CHANGE

> It is inevitable that personal privacy will be one of the most significant pressure points in our national fabric for most of the 1990s. Advancing technology, depersonalization of the workplace and other social environments, a growing population ... all can be expected to create a greater personal need for a sense of space and dignity.
>
> Erwin Chemerinsky[27]

Introduction

This chapter will present the views and opinions of:

- special interest groups (e.g., Electronic Frontier Foundation, Computer Professionals for Social Responsibility, National School Board Association),
- legal scholars (e.g., Louis Brandeis, Michael Godwin, Ethan Katsh, Carl Kadie, Philip Miller),
- law school professors (e.g., Laurence Tribe, Dean Prosser, Daniel Burk, Frank Easterbrook, Henry Perritt), and,
- authors from scholarly publications (e.g., Harvard Law Review).

An Overview

Plans and Policies,[28] a National School Board Association guide to formulating AUP statements, suggest that AUPs should foster "Intellectual Freedom

---

[27] Quoted in Josh Kratka. (1990). For their eyes only: The insurance industry and consumer privacy. Boston: Massachusetts Public Interest Research Group, page 1.

[28] Institute for Transfer of Technology to Education. (1995). Plans and policies for technology in education. Washington, DC: National School Boards Association.

... [as there is a need for a computer network to] be a free and open forum for expression that is strange, unorthodox, or unpopular."[29] However, this philosophy has already been pre-empted in other parts of the chapter where the authors advocate that an AUP should state that users should:

- "Avoid offensive or inflammatory speech,"[30] and,
- "[Avoid s]ending material that is likely to be offensive or objectionable to recipients ..."[31]

It becomes apparent in Plans and Policies that there has been a great deal of thought and effort put into justifying the use of computer networks in Education (e.g., parental permission forms, parental information advisories). But the policy concepts tend not to be based upon the U.S. Constitution, federal and state laws, judicial opinion, and institutional policy. It may be argued that "an AUP is a contract between the institution and the computer user. It may also be argued that if it is permissible for a person to waive or bargain away the right to privacy, then the only question that remains is whether the contractual negotiations were proper (e.g., was the user fully informed, not under coercion or duress, etc.)."[32]

Advocacy for AUP statements which lack a fair and equitable foundation is not limited to textbooks or existing institutional AUPs. The U.S. Supreme Court does not have a particularly strong record when dealing with Constitutional issues as

---

[29] Institute for Transfer of Technology to Education, page 36.
[30] Institute for Transfer of Technology to Education, page 33.
[31] Institute for Transfer of Technology to Education, page 38.
[32] Daniel Burk (personal e-mail, April 6, 1996).

they relate to new technologies.[33] "In addition, [lower] courts sometimes have a disturbing tendency to treat regulations of the electronic media as principally structural economic regulations without recognizing the effects on [Constitutional] values."[34]

The Supreme "Court often succumb[s] to the temptation to analogize (map[35]) new electronic media to existing technologies for which they have already developed [Constitutional] models."[36] For example, in Los Angeles v. Preferred Communications Justice Blackmun, in his concurring opinion, stated that: "In assessing [Constitutional] claims concerning cable access, the Court must determine whether the characteristics of cable television make it sufficiently analogous to another medium to warrant application of an already existing standard, or whether those characteristics require a new analysis."[37] "Academic commentary also often sets out the existing regulatory models—print broadcasting, and common carrier—

---

[33] Compare Mutual Film Corp. v. Industrial Comm'n, 236 U.S. 230, 244 (1915) (stating that motion pictures "[are] not to be regarded . . . as part of the press of the country") with United States v. Paramount Pictures, Inc., 334 U.S. 131, 166 (1948) (observing that "moving pictures . . . are included in the press whose freedom is guaranteed by the First Amendment").

[34] Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994).

[35] Since the inception of networked computer systems analysts have attempted to scrutinize the rights and duties of participants in these systems by analogizing an event in Cyberspace and applying a legal metaphor. This analysis is based upon the application of real life laws to a, more or less, equivalent, happening on a networked computer system. For example, one may consider e-mail to 'map' onto, or metaphorically be akin to, postal mail. Still others may consider e-mail to 'map' onto legal standards inherent to a telephone call.

[36] Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994).

[37] Los Angeles v. Preferred Communications, Inc., 476 U.S. 488, 496 (1986).

and then tries by analogy to fit a new media technology into one or more of the old models."[38] Marks and Johnson note:

> Any attempt to map territory that is unstable, unknown and changeable proves to be difficult, which is why metaphors, which are like maps, do not help in any consistent way. Instead one needs a guide to maneuver through the difficult areas... In other words, the best way to determine the rights and duties of the participants in electronic networking communities is not to pick a particular metaphor to be our map, but rather, to apply basic principles of fairness and justice and to use the existing 'legal metaphors' only for what they are worth as illuminators of a principled discussion.[39]

On the other hand, Miller argues that: "computer electronic information services are analogous to print publishers."[40] Indeed, sometimes the Constitutional treatment of the new medium hinges on which analogy the court adopts.[41]

Often, the process of analogizing has focused on the technological similarities of the different media.[42] "Technological characteristics, however, should not be the crucial factor in determining the protection a message receives under the [U.S. Constitution]."[43] The courts and those who craft AUPs "should ground [their] analysis in essential [Constitutional] interests and draw upon salient technological

---

[38] Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994).

[39] David R. Johnson and Kevin A. Marks, Mapping Electronic Data Communications Onto Existing Legal Metaphors: Should We Let Our Conscience (And Our Contracts) Be Our Guide?, 38 Villanova L. Rev. 487, 488 (1993).

[40] Philip H. Miller, Note, New Technology, Old Problem: Determining the First Amendment Status of Electronic Information Services, 61 Fordham L.Rev. 1147, 1190-91 (1993).

[41] Compare Midwest Video Corp. v. FCC, 571 F.2d 1025, 1056 (1978), aff'd, 440 U.S. 689 (1979) (overturning access regulations in part because cable television is indistinguishable from newspapers) with Berkshire Cablevision, Inc. v. Burke, 571 F.Supp. 976, 986 (1983), vacated, 773 F.2d 382 (1985) (upholding access regulations in part because cable service is analogous to broadcasting).

[42] E.g., Telecommunications Research & Action Center v. FCC, 801 F.2d 501 (1986), cert. denied, 482 U.S. 919 (1987) (The D.C. Circuit held that the FCC could not refuse to apply regulations that are constitutionally permissible for broadcasting to teletext.) Teletext is the functional equivalent of print, except that the text appears on a television screen instead of a sheet of paper. The court, however, found the technological analogy to broadcasting to be dispositive: "Teletext, whatever its
similarities to print media, uses broadcast frequencies, and that, given Red Lion, would seem to be that." Id.; See also, Red Lion Broadcasting Co. v. FCC, 395 U.S. 367, 386 (1969).

[43] Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994).

characteristics only as the factual background against which the real [Constitutional] concerns must be applied … [and the] Constitution's norms, at their deepest level, must be invariant under merely technological transformations."[44]

Judge Easterbrook,[45] in his comments regarding how the legal community is trying to set doctrine in order to come to a conceptual understanding of a computer network, bemoans the "cross-sterilization of ideas"[46] by combining the field of law with that of computer science. He states that doing this yields the "worst of both worlds."[47] Easterbrook notes that the belief "lawyers hold about computers, and the predictions they make about new technology, are highly likely to be false. This should make us hesitate to prescribe legal adaptations for cyberspace."[48]

The Executive Branch of the federal government has also taken action to confuse the legal concept of on-line computer networks. In 1987, for example, when "Congress tried to eliminate the NSA's [(National Security Agency)] meddling with civilian computers by passing the Computer Security Act … [the Act] was subverted by a series of Presidential directives and agreements among [White House] departments."[49]

Given the changing demographics of the on-line community, developers, enactors, and enforcers of AUPs should have a firm conceptual and legal understanding of the scope and limits of privacy as defined by court decisions,

---

[44] Laurence H. Tribe. (1991, March). The Constitution in cyberspace: Law and liberty beyond the electronic frontier. Keynote address at the First Conference on Computers, Freedom and Privacy, Boston, MA. Available as of July 1, 1996: http://www.swissnet.ai.mit.edu/6095/articles /tribe-constitution.txt.

[45] Judge Frank H. Easterbrook, United States Court of Appeals for the Seventh Circuit, and Senior Lecturer, The Law School, The University of Chicago.

[46] Frank H. Easterbrook. (1995, November). Cyberspace and the law of the horse. Paper presented at the University of Chicago Legal Forum's Symposium on the Law of Cyberspace, Chicago, Illinois. Available as of July 1, 1996: http://www-law.lib.uchicago.edu /forum/easterbrook.doc.

[47] Frank H. Easterbrook. (1995, November). Cyberspace and the law of the horse.

[48] Frank H. Easterbrook. (1995, November). Cyberspace and the law of the horse.

[49] Press Release from the Electronic Freedom Foundation dated March 5, 1996.

legislation, and applicable campus policy. As a result of this change in the nature of the user base, a university now needs to set policy and provide a policing function in regard to the on-line computer network much in the same manner that it should set policy and provide policing of activities on the real life campus.

The Right to Privacy--Warren and Brandeis' Thesis

The Harvard Law Review of December 1890 contained an article written by Samuel Warren and Louis Brandeis,[50] titled *The Right to Privacy*, which described the right to privacy as "the right to be let alone."[51] The writing of this article was prompted by Samuel Warren's outrage in regard to a gossip column reporter's comments about a family wedding.[52] This article has been a widely quoted seminal contribution to the law. According to Shapiro, The Right to Privacy is the most cited law review article.[53]

Warren and Brandeis touch upon principles which are being revisited today in regard to rights on computer networks. When Warren and Brandeis pondered the issues of their day the same legal tenets applied. In 1960, William L. Prosser strengthened Brandeis and Warren's theory by publishing an article[54] in the California Law Review tracing more than 300 cases germane to the evolution of the right to

---

[50] Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, (1890).
[51] Warren and Brandeis at 193.
[52] Dianne L. Zimmerman, Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort, 68 Cornell L.Rev. 291, 295-96 (1983).
[53] Shaprio, Fred R. (1987). The most cited law review articles. Buffalo, NY: W. Hein Co.
[54] Dean Prosser, Privacy, 48 Cal. L. Rev. 383 (1960).

privacy.[55] The influence of the works of Warren and Brandeis, and Prosser, contributed greatly to the recognition of the right of privacy. Today, we are dealing with computer technology moving beyond the current scope and understanding of existing statutes. In their day Warren and Brandeis were confronted with similar issues—expanding the understanding needed to craft/broaden statutes to accommodate new technology. It is therefore quite important to revisit this seminal law review article and follow Warren and Brandeis's lines of reasoning so that we may apply their thinking to today's quandaries and dilemmas.

When our nation began, the law only provided legal remedy for actual "physical interference with life and property, for trespasses *vi et armis*."[56] Warren and Brandeis believed that the concept that the "individual [should] have full protection in person and in property is a principle as old as the common law."[57] They also state that it is necessary "from time to time to define anew the exact nature and extent of such protection."[58] Warren and Brandeis were attempting to lay a foundation to allow the existing legal philosophy to grow to accommodate changing circumstances and specifics. "Gradually, the scope of these legal rights broadened and, now, the right to life has come to mean the right to enjoy life--the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the

---

[55] William C. Bier. (1980). Privacy: A vanishing value? New York: Fordham Univ. Press, page 93.

[56] Warren and Brandeis at 193.

[57] Warren and Brandeis at 193.

[58] Warren and Brandeis at 193.

term 'property' has grown to comprise every form of possession—intangible, as well as tangible."[59]

The Right to Privacy of the Modern Day

> Uses of new technologies raise policy issues that are often defined in terms of invasion of privacy.[60]

A problem in legislating policy to define and protect privacy is that it is difficult to conceptualize privacy. Authors of philosophical and legal works about privacy emphasize that their subject is difficult to define.[61] Alan Westin's book Privacy and Freedom begins: "Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists."[62] Judith Jarvis Thompson's article "The Right to Privacy" opens: "Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is."[63] Similarly, C. Herman Pritchett, in his forward to David O' Brien's book Privacy, Law, and Public Policy states: "Privacy is a confusing and complicated idea."[64] "These difficulties in conceptualizing privacy not only are of philosophical importance but also have profound implications for the formulation of public policy to protect privacy ."[65] In the American tradition, there are "two types of rights—civil liberties and civil rights. Privacy is defined as a civil liberty—a right to be free of outside interference,"[66] or as

---

[59] Warren and Brandeis at 193.

[60] Priscilla M. Regan, (1995). Privacy, technology, and public policy. Chapel Hill, NC: University of North Carolina Press, page 2.

[61] Regan, page 3.

[62] Alan Westin. (1967). Privacy and freedom. New York: Anthenum Press, page 3.

[63] Judith Jarvis Thompson. (1995, Summer). The right to privacy. Philosophy and Public Affairs, 4(4), page 4.

[64] David M. O'Brien. (1979). Privacy, law, and public policy. New York: Praeger, page vii.

[65] Regan, page 4.

[66] Regan, page 5.

Berlin terms it, a "negative liberty."[67] Vincent Samar also makes the point that "legal privacy is a species of negative freedom."[68]

Defining a problem in terms of rights has been a potential resource for many issues civil rights, women's right, rights of the disabled--but these issues involve rights to some benefit of status and are defined not in terms of an atomistic individual but an individual as a member of a group.[69] Because privacy is seen as an individual interest and choice, ambiguities about its meaning exist. It is assumed that different people define privacy differently. Tien notes that "[p]rivacy can be a huge can of worms ...analyzing it as a conceptual problem ...often becomes a mess of conflicting statements that everyone agrees on."[70]

Privacy, among other things, is a benchmark when dealing with search and seizure processes. Understanding the issue of search and seizure is also critical when attempting to develop an understanding of on-line computer networks, because search and seizure occupies an antithetical legal position[71] to privacy.

A number of advocacy groups have been formulated to address electronic issues. The Electronic Frontier Foundation (EFF),[72] the Computer Professionals for

---

[67] Isaiah Berlin, Two concepts of liberty, in Four essays on liberty. (1969). London: Oxford University Press, page 118-172.

[68] Vincent Samar, (1993). The right to privacy: Gays, lesbians, and the constitution. Philadelphia, PA: Temple University Press, page 53.

[69] Regan, page 4.

[70] Lee Tien (personal e-mail, March 17, 1996).

[71] John M. Junker, The Structure of the Fourth Amendment: The Scope of the Protection, 79 Crim. L. & Criminology 1105, 1177 (1989) (The Fourth Amendment balances and individual's claim to privacy against society's need to control crime or to generally its right to 'know'). Also see, Jones v. United States, 362 U.S. 257 (1960) (Adopted the rule that the person challenging the legality of a search and seizure must have been a "victim."); Rankas v. Illinois, 439 U.S. 128 (1978) (Tightened the Jones ruling to require that a person have a "legitimate expectation of privacy" in the area searched or the material seized).

[72] The Electronic Frontier Foundation (EFF) was founded in July of 1990 to ensure that the principles embodied in the Constitution and the Bill of Rights are protected as new communications technologies emerge. EFF's AUP archives are located at http://www.eff.org/policy.

Social Responsibility (CPSR),[73] and on a smaller scale, the National Center for Technology Planning[74] maintain a compendia of AUPs and AUP related documents which provide an excellent starting point for research. The AUP documents located at these sites provide sources for investigation of the state of AUPs across the country.

A preliminary review of these documents confirms the notion that AUPs have been, and continue to be, constructed based upon an outdated perception of the nature of an on-line computer network.[75] There is a conspicuous lack of legal foundation (e.g., studies and discussions of Constitutional principles and laws, existing campus policy, and judicial decisions) in existing AUPs. Many of the AUP policy statements now being enacted look and feel as though they are legal. But upon examination they appear to lack substantive legal foundation. For example, Dr. Carl Kadie has overlaid a university's AUP onto the rules of its real world campus, and wondered what an uproar there would be if the university rules paralleled the pronouncements within the AUP:

> * The University has the power to, without notice, inspect any assigned office space or dorm room.

---

[73] The Computer Professionals for Social Responsibility (CPSR) was founded in 1981. The CPSR is a group of concerned computer scientists in Palo Alto, California, who worked to implement social responsibility among computer professionals by forming a discussion group and then a national network of computer professionals and users to advocate for the responsible use of computer technology and encourage all who use computer technology to participate in the public debate.

[74] The National Center for Technology Planning (not an agency of the federal government or any national organization) maintains a compendium of AUPs. Available as of July 1, 1996: http://www.scholastic.com.

[75] In past years, on-line computer systems were utilized for research by scientists. These scientists were very like-minded as to the uses and etiquette that were appropriate. More recently, on-line systems are being utilized by a highly diverse general-public. This usage by a diverse general public is generating a need for rules that reflect the real world.

> * Members of the University community may NOT distribute or make accessible offensive or annoying material.
> * Members of the University community may be punished for infractions against rules that are NOT listed here.
> * Members of the University community must not "use University property," where "mis-using University property" is defined as misusing University property.
> * The University has the power to "amend the Conditions and Policies at any time without prior notice."[76]

In addition, the concept of "University property"[77] (as cited above) needs to be examined. Among other things, the concept itself is vague and overly broad. More generally, what is "at issue are the 'authority-conferring' concepts—misuse of property, for example—and the invasions of privacy that are *prima facie* justified by them."[78]

The due process[79] aspect also appears to be faulty. For example, the University has reserved the power to "amend the Conditions and Policies at any time without prior notice."[80] This appears to strip an offender of the right to due process. It also appears to strip away the concept of publishing the rules so that the users may know the standards to which they will be held accountable.

Search and Seizure Issues

A public university AUP should also address search and seizure issues. There will be occasion for university officials to intrude into user accounts. Therefore, it is important for university officials to base their AUP on sound search and seizure theory as they may need to justify a 'search' or a 'search and seizure', or, they may

---

[76] Boston University AUP [Online]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies. Dr. Kadie has revised the BU AUP to read as though it were the policy for the real world campus.

[77] Carl Kadie (personal e-mail, July 1, 1996).

[78] Lee Tien (personal e-mail, March 17, 1996).

[79] Palko v. Connecticut, 302 U.S. 319 (1937) (Due Process does not have does not have a fixed meaning but it expands with jurisprudential attitudes of fundamental fairness).

[80] Boston University AUP [Online]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies. Dr. Kadie has revised the BU AUP to read as though it were the policy for the real world campus.

need to justify the basis upon which other disciplinary action is taken. Also such policy should strive to enforce itself by the least restrictive means possible.

In recent years computer systems have been seized as evidence when only seizure of a copy of the offending material was in order.[81] Absent an understanding of First Amendment and Fourth Amendment principles that are applicable to on-line computer networks, law enforcement officials have caused search warrants to be issued that are overly broad.[82]

Kapor and Godwin warn of computer searches and seizures based upon the American Bar Association's (ABA) Criminal Justice Section suggested search and seizure guidelines.[83] They are concerned that the ABA's position seems to be based upon three publications[84] from the U.S. Department of Justice, which seem to skew the principles involved in searches and seizures toward law enforcement's position instead of providing a balance between the public's right to know and the individual's right to have privacy.

Commenting further upon this issue, Kapor and Godwin note that the American Bar Association's (ABA) Criminal Justice Section suggested search and seizure guidelines are faulty because:

---

[81] Fed. R. Evid. Rule 101(3) holds that an "original" can be "any print-out or other output readable by sight [and] shown to reflect the data accurately," which has been taken from a "computer or similar device."

[82] Dibbell. (1990, July 24). On line and out of bounds. Village Voice, page 27; Jahnke. (1990. November 14). The cops come to cyberspace. Boston Magazine; John P. Barlow. (1990). Crime and puzzlement [On-line]. Available as of July 1, 1996: http://www.eff.org/pub/Publications /John_Perry_Barlow/crime_and_puzzlement.1. See also, Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (May, 1995).

[83] Mitchell Kapor and Michael Godwin. (1994). Civil liberties implications of computer searches and seizures: Some proposed guidelines for magistrates who issue search warrants [On-line]. Available as of July 1, 1996: http://www.eff.org/pub/Publications/Mike_Godwin /search_and_seizure_guidelines.eff.

[84] J. McEwan. (1989). Dedicated computer crime units. Washington, DC: National Institute of Justice.; D. Parker. (1989). Computer crime: Criminal justice resource manual. Washington, DC: National Institute of Justice; C. Conly. (1989). Organizing for computer crime investigation and prosecution. Washington, DC: National Institute of Justice.

> There was no guidance to the magistrate as to when the computer or related equipment should not be seized, either because it is not necessary as evidence or because such a seizure would intolerably "chill" the lawful exercise of First Amendment rights or abridge a property owner's Fourth Amendment rights.
>
> There was inadequate recognition of the business or individual computer owner's interest in continuing with lawful commercial business, which might be hindered or halted by the seizure of an expensive computer.
>
> There was no effort to measure the likelihood that investigators would find computers equipped with such justice-obstructing measures as automatic erasure software or 'degausser' booby-trapped hardware, the presence of which might justify a 'no-knock' search and seizure, among other responses.[85]

One difficulty is that law enforcement agencies have only attempted to discern what the misuses of a computer are. This creates a situation where law enforcement agencies do not routinely recognize First and Fourth Amendment significance of on-line computer networks and other forms of electronic speech and publishing. The resulting problem is that there is a tendency to issue broad search and seizure warrants. Warrants issued based on this line of thought can, in the long term, abridge a person's First Amendment rights.

Sergent notes that there is still a compelling need to formulate a search and seizure model for computer networks to protect privacy. He states that a question "of user privacy arises when examining [a search] warrant's scope. Search warrants should be restricted to the files under investigation. A warrant's scope should not allow invasion of privacy interests of individuals..."[86]

---

[85] Mitchell Kapor, and Michael Godwin. (1994). Civil liberties implications of computer searches and seizures: Some proposed guidelines for magistrates who issue search warrants [On-line]. Available as of July 1, 1996: http://www.eff.org/pub/Publications/Mike_Godwin /search_and_seizure_guidelines.eff.

[86] See generally, Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (May, 1995). Also see, Terri Cutrera, Note, The Constitution in Cyberspace: The Fundamental Rights of Computer Use, 60 U.M.K.C. L. Rev. 139 (1991).

To add to the blurring of the legal landscape, there are a number of gaps in statutes created by the technology itself. This is evident where there is no applicable statute, or there are conflicting statutes.[87] For example, in LaMacchia[88] "the question of whether the defendant had in fact committed any crime at all turned out to be a difficult [question] for authorities to answer."[89] LaMacchia's attorney, Harvey A. Silverglate stated that: "The government attempts to assert control over this burgeoning thing called the Internet [from time to time] ... [and] spasmodically overreacts in order to set an example, to deter behavior the government doesn't like,"[90] which then leads to misapplication of the law.

To compound the lack of clarity and definition on the computer-legal frontier, Congress passed the Communications Decency Act[91] (CDA) as part of the telecommunications reform bill in February 1996. The CDA would have imposed huge fines and prison terms on anyone who sends or displays 'indecent' or 'patently offensive' material in a public forum on the Internet. There was a challenge to the

---

[87] David R. Johnson and Kevin A. Marks, Mapping Electronic Data Communications Onto Existing Legal Metaphors: Should We Let Our Conscience (And Our Contracts) Be Our Guide?, 38 Villanova L. Rev. 487, 488 (1993).

[88] United States v. David M. LaMacchia, Criminal No. 94-10092RGS, March 1994.

[89] Mike Godwin. (1995, March). No copycat criminal: LaMacchia case reveals a federal attitude problem. Internet World. Available as of July 1, 1996: http.//swissnet.ai.mit.edu/6095 /readings-crime.html#Required

[90] Harvey A. Silverglate, Silverglate, Harvey A. (1994, December 24). Statement of Silverglate and Good concerning the dismissal of the indictment in United States v. David M. LaMacchia. Available as of July 1, 1996: http://www.swissnet.ai.mit.edu/6095/articles /dml/lamacchia.html.

[91] Telecommunications Act of 1996, 47 U.S.C §151 (1996).

law,[92] and in June of 1996 a special three judge panel in Philadelphia ruled the CDA unconstitutional. Currently this issue is headed to the Supreme Court for resolution.

The lack of understanding as to the nature of on-line computer networks is seen at the state level also. Easterbrook notes that "[e]rror in legislation is common, and never more so than when technology is galloping forward."[93] In New York, for example, the state legislature is considering the passage of telecommunications legislation which seems to ignore fundamental Constitutional issues.[94]

> Law is a process that is oriented around working with information. As new modes of working with information emerge, the law cannot be expected to function or to be viewed in the same manner as it was in an era in which print was the primary communications medium. Nor can the law be expected to support the same symbols and metaphors.[95] Not only the seamless web, but "fine print," "black letter law," "law on the books," "going by the book," and other print based

---

[92] The ACLU, the CPSR and 19 other plaintiffs have initiated a lawsuit to challenge the constitutionality of the Communications Decency Act (CDA) on grounds that it flagrantly suppresses First Amendment rights. A Federal court issued a Temporary Restraining Order on Feb. 8, 1996 barring the enforcement of part of the CDA. The court stated that the CDA will have a chilling effect on free speech on the Internet and found that the CDA raises "serious, substantial, difficult and doubtful questions." The court further agreed that the CDA is "unconstitutionally vague" as to the prosecution for indecency.

[93] Frank H. Easterbrook. (1995, November). Cyberspace and the law of the horse. Paper presented at the University of Chicago Legal Forum's Symposium on the Law of Cyberspace, Chicago, Illinois.

[94] Update on New York State Bill. (1996, February 18). BillWatch. Available as of July 1, 1996: http://www.vtw.org/billwatch (New York Internet, a business oriented Internet Service Provider in New York state, suggested that New York State Internet bill (S210/A3967) was poorly drafted as it had major Constitutional flaws and conflicted with existing statutes. The major problems were: a. inappropriate liability for Internet providers, b. criminalization of speech that is currently legal in print, and, c. no mention of the plethora of parental control tools).

[95] Milner S. Ball. (1985). Lying down together: Law, metaphor and theology. Madison, WI: University of Wisconsin Press, page 21-36. The author suggests that current metaphors of law as bulwark of freedom promote "order" rather than "justice."

Many metaphors have been offered in attempts to capture the nature and meaning of an on-line computer network. An on-line computer network is analogous to many familiar real-life metaphors, not just to one. It is analogous to a: newspaper, republisher/disseminator, common carrier (e.g., telephone company), traditional bulletin board (the wood and cork type), broadcaster, desk at the office, desk at home in the den, free and open frontier (a.k.a. *The Old West* of the 1800s), safe deposit box in a bank, hotel/motel room which one has rented, fraternity/sorority house. Depending on which metaphor is invoked, the legal perspective of a computer account will vary greatly.

> expressions will be replaced by allusions that are more consistent with the qualities of law and information in electronic form.[96]

In addition to the gaps being created by this new on-line electronic technology a legal and ethical blurring is occurring due to the lack of consensus among the various stakeholders as to what legal metaphors[97] apply.

Perritt notes that: "In the long run, adoption of information technologies will blur the boundaries between citizen and agency and between agency and court. Blurring of these boundaries may necessitate rethinking the definitions of some of the basic events that define the administrative process, public participation and judicial review."[98]

Presently, for example, "the balance between speakers' rights and listeners' privacy interests depends largely on how courts conceptualize the forum in which the speech takes place."[99] If the Information Superhighway is regarded as analogous to public space then First Amendment principles evident outside of the electronic media suggest that the burden may be on users of the information superhighway to avoid unwanted messages by electronically averting their eyes.[100] In other words, accessing

---

[96] Ethan Katsh. (1995). Law in a digital world. New York: Oxford University Press, page 406.

[97] George Lakoff and Mark Johnson. (1980). Metaphors we live by. Chicago: University of Chicago Press, page 139. " [M]etaphors are capable of giving us a new understanding of our experiences. Thus we can give new meaning to our past, to our daily activity, and to what we know and believe." Also see, James B. White, The legal imagination, page 57-64. "As [the lawyer] works on an antitrust or criminal appeal, the lawyer may say to himself that what he is doing and saying really means something else . . . The activity of law can be spoken [of] in other terms."

[98] Henry A. Perritt Jr., The Electronic Agency and the Traditional Paradigms of Administrative Law, 44 Admin. L. Rev. 79 (1992).

[99] Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994).

[100] Laurence Tribe, American constitutional law.

the information superhighway may be analogous to walking onto a city street, and computer network users may be expected to cope with the wide array of entertainment, annoyance, and offensive acts that normally takes place in the real world, or, it may be deemed to be analogous to one's home which would shift the burden away from the viewer.

There is also a lack of familiarity with that place known as cyberspace. This lack of mature experience during this period of development introduces yet another complicating factor in the rapidly evolving nature of the environment. For example, commercial transactions are being transplanted onto this electronic medium that is basically focused on communication. The question is arising as to whether the medium imbues commercial activities with First Amendment or any other Constitutional protections. "That is, if a non-First Amendment activity such as a bank transaction occurs over a communications medium, is the First Amendment implicated?"[101] The Internet, or as it has become known, *Information Superhighway*[102] is blurring the distinctions with which we have become familiar.[103] Interactivity will make it difficult to differentiate *the transaction* from *speech* that

---

[101] See Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 564 (1980).

[102] *Information Superhighway* is a term initially popularized by then-Senator Albert Gore. See Albert Gore, (1990, July 15). Networking the future: We need a national "superhighway" for computer information. Washington Post, page B3.

[103] Other changes in the economy are likely to put added pressure on the distinction between speech and economic transactions. In particular, the growing importance of information as a commodity that is bought and sold may raise First Amendment concerns in the context of economic transactions.

concerns the transaction.[104] To the extent that these two activities become indistinguishable, courts may have to apply at least a minimal First Amendment standard to activities that were previously clearly outside the reach of the First Amendment.[105] The speech-conduct distinction may therefore result in blurring of economic activities as well as of expressive ones.

Bruce Sterling states that: "Cyberspace demand[s] a new set of metaphors, rules and behaviors."[106] During the time while legal scholars and legislatures explore, study and eventually enact legislation, the university should account for this lack of statutory guidance. The legislatures and the courts may decide to enact legislation or view cases in such a manner that, *de facto*, the university will be charged with the task of defining foundational doctrine which defines their AUP.

In addition, a current-day AUP should define the computer user's rights and responsibilities to the system itself, to other users, and to the administrators of that system. The AUP should also define the administration's rights and responsibilities to the system itself, and to the users of that system. It appears that this may be a responsibility which should be represented in the AUP, rather than a judicial concern. As a result, the university AUP, among other things, may need to embody legal

---

[104] Although home shopping channels exist today, the degree of intermingling of commercial speech and activity is considerably different. These channels in effect advertise the product and allow the consumer to buy almost immediately. The transaction itself, however, occurs through another medium--the telephone. This provides at least an initial dividing line between the commercial speech and the actual transaction.

[105] Charles Fried, Constitutional Doctrine, 107 Harv. L. Rev. 1140, 1154 (1994) ("In recent years, it has become evident that information is becoming one of the most important items of commerce, or more broadly, of production, exchange, and consumption, so that constitutional protection for liberty of expression and information may be the route by which once again the Constitution is invoked to protect broad lines of economic activity from government regulation.")

[106] Bruce Sterling. (1995). The hacker crackdown. New York: Bantam Books, page 208.

Current practice in crafting the AUP should be directed to accommodate:

- a concern for the human interactions which occur on the computer system,
- the software's capabilities to manage those interactions, and,
- the applicable Constitutional concepts, laws, and judicial opinions.

These concerns translate into Acceptable Use Policy frameworks, which among other things, are intended:

> (1) to educate the University community to the opportunities and obligations inherent in a pervasive digital networked environment, and (2) to make information as accessible and useful as possible to the University's various constituencies. These goals can be met only if the individual units are guided by a consistent philosophical framework for establishing policies and practices.[107]

Summary

> Technological change often outpaces the law. Examining the legal implications of emerging technologies can help narrow this gap. Although the precise contours of the new media technologies are not yet known, certain radical evolutions in the way we receive, transmit, and utilize information have already become apparent.[108]

The possibilities engendered by the Information Superhighway will evolve in many ways. "Two evolutions—infinite choices and interactivity—will have profound impact"[109] on, *inter alia*, the need to revisit Constitutional issues in order to reassess their application to user policy issues. This reality is beginning to impact federal legislators. This is a positive event and we can look forward to a coherent national policy regarding the nature of cyberspace. But until that time, those who must create

---

[107] William Graves, Carol Jenkins and Anne Parker. (1995, Summer). Development of an information policy framework. Cause/Effect, page 15.

[108] Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994). See generally, Anne M. Fulton, Cyberspace and the Internet: Who Will Be The Privacy Police?, 3 Comm. Law Conspectus 63 (1995).

[109] Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994).

their application to user policy issues. This reality is beginning to impact federal legislators. This is a positive event and we can look forward to a coherent national policy regarding the nature of cyberspace. But until that time, those who must create institutional Acceptable Use Policy should develop their own understanding of what constitutes fair and equitable policy in this environment which has warped our sense of the law.

Harvard law professor and Constitutional scholar Laurence Tribe posed this question: "When the lines along which our Constitution is drawn warp or vanish, what happens to the Constitution itself?"[110] A possible answer to Professor Tribe's question is: 'As a blurring of legal definition occurs, a university should identify and revisit the basic conceptual issues inherent in an AUP.' And, a root concept appears to be that of the right to privacy.

Privacy is a major issue of our day. As Smith states: "There seems to be no legal issue today that cuts so wide a swath through conflicts confronting American society [as Privacy]. From AIDS tests to wiretaps, polygraph tests to computerized data bases, the common denominator has been whether the right to privacy outweighs other concerns of society . . ."[111] A Louis Harris poll (figure 3) supports the position that Privacy, the root of a number of present issues, is a significant concern of the American people.

---

[110] Laurence H. Tribe. (1991, March). The Constitution in cyberspace: Law and liberty beyond the electronic frontier. Keynote address at the First Conference on Computers, Freedom and Privacy, Boston, MA. Available as of July 1, 1996: http://www.swissnet.ai.mit.edu/6095/articles /tribe-constitution.txt.

[111] Robert Ellis Smith. Quoted in Andre Bacard. (1995). The computer privacy handbook. Berkeley, CA: Peachpit Press. page 17.

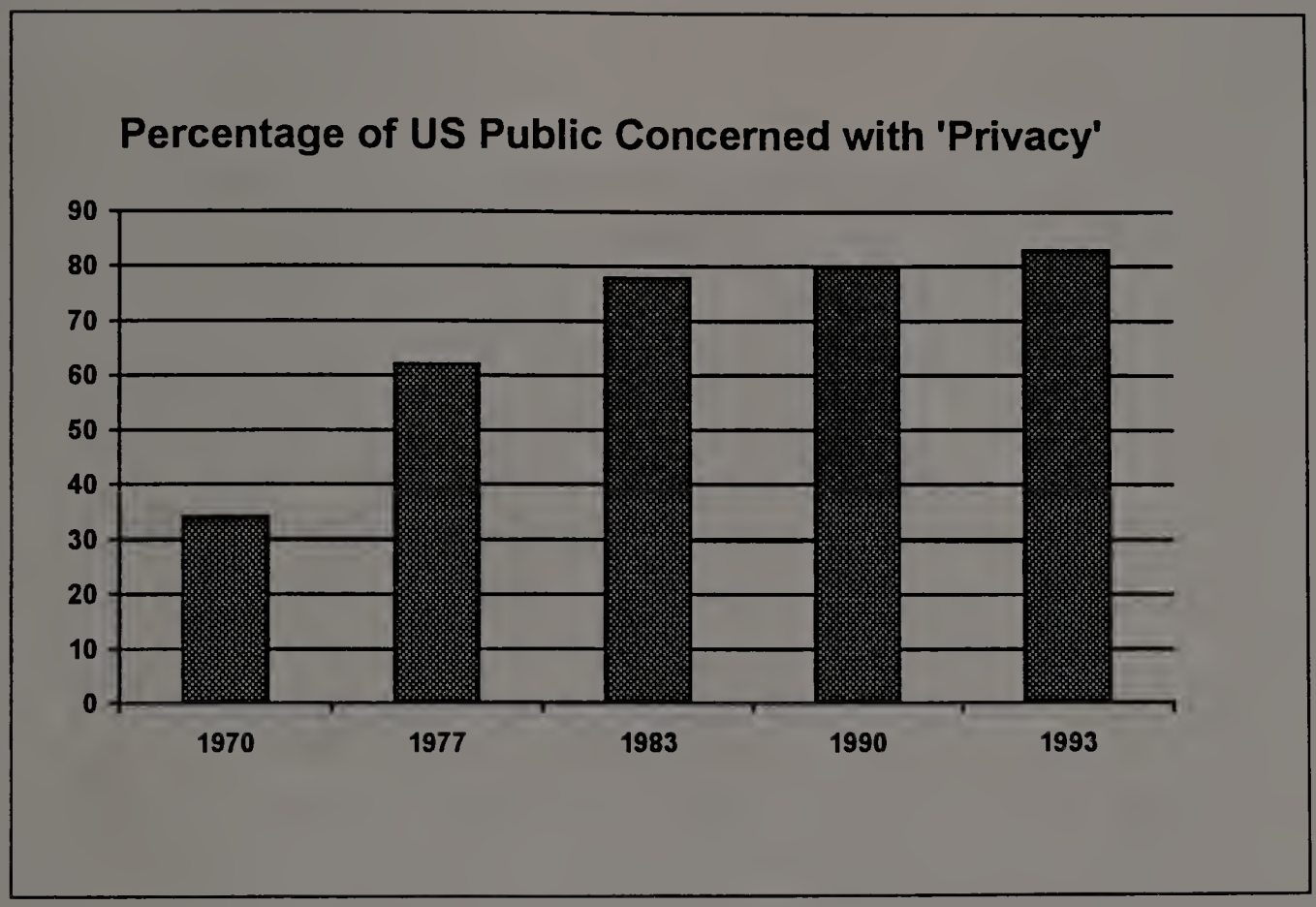

Figure 3 - 1993 Louis Harris Poll regarding Public Perception of Privacy[112]

Drawing models of privacy and search and seizure with the intent of applying them to Acceptable Use Policies may not be realistically possible.[113] Easterbrook[114] and de Sola Pool[115] suggest that looking to our legal system for guidance is not yet

---

[112] A 1993 poll conducted by Louis Harris and Associates. Also see, The Equifax Report on Consumers in the Information Age, conducted by Louis Harris Associates and Dr. Alan Westin (1990); and Equifax Inc., Harris-Equifax Consumer Privacy Survey 1991 and Harris-Equifax Consumer Privacy Survey 1992. The question posed in all these surveys was -- "How concerned are you about threats to your personal privacy in America today?" The graph reflects those respondents who indicated that they were either 'very concerned' or 'somewhat concerned'.

[113] David R. Johnson and Kevin A. Marks, Mapping Electronic Data Communications Onto Existing Legal Metaphors: Should We Let Our Conscience (And Our Contracts) Be Our Guide?, 38 Villanova L. Rev. 487, 488 (1993).

[114] Frank H. Easterbrook. (1995, November). Cyberspace and the law of the horse. Paper presented at the University of Chicago Legal Forum's Symposium on the Law of Cyberspace, Chicago, Illinois. Available as of July 1, 1996: http://www-law.lib.uchicago.edu /forum /easterbrook.doc.

[115] Ithiel de Sola Pool. (1983). Technologies of freedom. Cambridge, MA: Belknap Press, page 7.

possible. The legal community is still in the process of analyzing the phenomenon known as cyberspace. They are in the process of setting doctrine which will legally define actions in cyberspace. Even with clear legal foundational guidance from the legislature and the courts, there may be specific concerns that will not be addressed by courts examining privacy and other Constitutional questions, but which will apply to the development of Acceptable Use Policies.

There is a need for universities to craft local rules for a computer network. It may also be a compelling reason for universities to craft their own AUP, because the AUP may, even for public institutions, "boil down to a matter of contract"[116] as they are in private institutions. Thus universities should research the issue of privacy as it applies to on-line computer systems. Even if an Acceptable Use Policy is eventually deemed to be a contract, there still remains a need to base the AUP upon the same concepts which are inherent in the U.S. Constitution.

---

[116] Daniel Burk (personal e-mail, April 6, 1996).

CHAPTER III

THE RESEARCH METHOD

> In the formulation of policy it is critical that the policy provide for security *and* access to information and communication while ensuring that the resource use does not overburden the system's capabilities. These conflicting demands must be analyzed and a synthesis arrived at. [117]

Introduction

In Chapter II, the review of the literature provided evidence that there exists a lack of clarity in regard to a number of legal rights when dealing with networked computer systems. Many existing and proposed statutes and AUPs are vague and overly broad. There also appeared to be a lack of a common understanding of the basic nature of an online computer network. This dissertation focused upon what the author considered to be a key foundational factor in the construction of an Acceptable Use Policy, that being the determination of the scope and meaning of user privacy.

Many of the issues inherent in the broader fabric of privacy (e.g., false light) do not appear to have immediate relevance on the issue of this study. But it is important to review them to gain an understanding of what the concept of privacy is and what it is not—and how these issues might be relevant to the formulation of an AUP, and how it might not be relevant.

---

[117] CAUSE Current Issues Committee. (1995, Summer). Current issues for higher education information resources management. Cause/Effect. Page 5.

The review of literature in Chapter II addressed the general right to privacy as defined by a line of decisions from the Supreme Court,[118] and also brought forth issues having to do with informational privacy. While informational privacy (having control of who can and cannot have access to information about one's bank accounts, pharmaceutical purchases, reading habits) is a very important issue, this study did not focus directly upon it. This formative research study did not focus upon the constitutional right of privacy which the Supreme Court has held to protect such activities as the use of contraceptives and the right to abortion. Rather, it focused upon a more narrow aspect of the notion *privacy*, and did address the right to privacy in the sense of one's right to have control over his/her computer account. This study also scrutinized the issues inherent in the rights that the system administrators have to invade the privacy of a user.

Overview

The research method utilized in this dissertation is not a traditional one. Neither an *opinion survey* nor a *random sample* is appropriate. In order to answer the questions inherent in this dissertation it is necessary to turn to a legal model of research. The legal model of research involves a careful review of statutes, law reviews, other scholarly legal publications, and on-line legal conferences.

---

[118] Although the term *privacy* is *not* mentioned in the US Constitution, it has been defined by the Supreme Court, through the years, in a line of decisions. The Court has held in Griswold v. Connecticut, 381 U.S. 479 (1965) that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create 'zones of privacy'. The right of association contained in the penumbra of the First Amendment is one..."); See also, Roe v. Wade, 410 U.S. 113 (1972) (The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, ... the Court has recognized

Assumptions/Research Questions

This dissertation attempted to determine the impact of certain aspects of the interpretation of the right to privacy to the formulation of an instutition's Acceptable Use Policy. The following questions and assumptions have been assessed:

1. The content of, and issues addressed by, existing Acceptable Use Policies.
2. The nature and philosophy of current AUP.
3. Current trends of thought on the part of legal scholars, law enforcement officials and advocacy groups.
4. The balancing of a computer user's right to privacy on a computer system with the university's right to insure the computer system functions properly.

Limitations of the Study

> Privacy can be a huge can of worms ... analyzing it as a conceptual problem ... often becomes a mess of conflicting statements that everyone agrees on.[119]

In all probability, the most important limitation of this study is the likelihood that the contours of the Internet and campus computer systems will not remain as they are today. Mark Luker, NSFNet Program Director, has stated that there will be an "Internet II" which will have greatly increased capability to perform tasks far beyond those of which the current Internet NSF is capable. Luker indicates that

---

that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution.)

[119] Lee Tien (personal e-mail, March 17, 1996).

"Internet II" will be far more interactive (video and audio interactivity), and, in the not to distant future, will be as ubiquitous as cable television is now.[120]

A possible source of difficulty in this study could be in the author's interpretation of certain statutes and/or case law. Even the most renowned legal and constitutional scholars do not all agree on the meaning, intent, or transferability of legal principles and case law. Therefore, the author's conclusions, which flow from those legal documents, analyses, discussions, and research/law review articles could be opened to other interpretations.

The contours of the author's opinions and conclusions may be altered by statutes and court decisions, as for example, "the balance between speakers' rights and listeners' privacy interests depends largely on how courts conceptualize the forum in which the speech takes place."[121] If, for example, the Information Superhighway is considered analogous to a public space,[122] then First Amendment principles suggest that the burden may be on users of the information superhighway to avoid unwanted messages by electronically averting their eyes.[123]

Depending upon the nature of Supreme Court or Congressional action(s), the shape of AUPs may not be in agreement with this study. For example, the

---

[120] Mark Luker (Interviewee). (1996, August 17). The future of the Internet. Washington journal [Television]. Atlanta, GA: Turner Network News, Inc.

[121] Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994).

[122] *Public space* here is not meant to be synonymous with *public forum*. *Public space* refers to space in which the public is relatively free to move about and interact, such as the courthouse in Cohen v. California, 403 U.S. 15 (1971). In order to be a public forum, public space must also have been traditionally open to all for expressive activities. See Edward J. Naughton, Is Cyberspace a Public Forum?: Computer Bulletin Boards, Free Speech, and State Action, 81 Geo. L. J. 409, 419-28.

[123] Laurence Tribe. American constitutional law (2d ed.). Mineola, NY: Foundation Press, page 1077.

Communications Decency Act (CDA) is contrary to the thinking of most legal scholars—parts of the CDA may even be contrary to the Constitution itself. While a Philadelphia federal circuit court has declared the CDA to be unconstitutional, the Supreme Court may reverse this decision. A Supreme Court reversal of the Philadelphia court's decision would cause a radical reshaping in the legal landscape of the Internet and university computer networks in regard to, *inter alia*, indecency.

Another possible difficult with this study is that the issue of privacy may not be as critical an issue in regard to the formulation of a university's AUP as the author has postulated.

The Methodology

By interrogating Lexis/Nexis with appropriate keywords and Boolean searches an attempt was made to survey the "lay of the land"[124] by examining law review articles and other scholarly publications pertinent to AUPs, privacy, and search and seizure.

Also, a general investigation of the state of Acceptable Use Policies (AUPs) across the country was conducted by searching web servers and ftp archives which contain collections of AUPs and AUP critiques.

This author explored the larger environment in which an AUP exists, since it is consequential to the development of an AUP to evolve a perspective of overarching issues which impact the use of networked computers (e.g. privacy issues, right of

---

[124] Nancy P. Johnson, Robert C. Berring and Thomas A. Woxland, Winning research skills (2nd ed. 1993).

access, freedom of speech, right of the administration to insure that someone does not break the system).

There was a subsequent focus on an exploration of a number of factors which the author considers important influences on the development of an understanding of the on-line environment in which privacy exists. It was essential to this study to research:

- the roots of the term privacy,
- privacy as a practical matter in the real world of today,
- philosophical issues surrounding privacy,
- privacy laws and judicial opinions concerning privacy in Massachusetts,
- existing Federal privacy-related statutes,
- privacy and the elements and requisites of liability,
- selected cases and statutes which map privacy decisions and statutes onto computer network issues, and,
- privacy in our electronic society.

The Fourth Amendment, which addresses the issue of search and seizure, impacts privacy as it, *de facto*,[125] forbids unreasonable invasion of that right to

[125] This only applies to public institutions as they are considered to be government actors. Private institutions are not included.

privacy. Therefore, the next phase of this study researched the nature of search and seizure. This was appropriate, as privacy and search and seizure occupy antithetical legal positions.

Kapor and Godwin[126] have stated that there appears to be immature search and seizure guidance from the courts, and from legislative bodies. Pursuant to Kapor and Godwin's statements, it is appropriate to survey the foundation issues involved in search and seizure. This study will:

1. investigate privacy and possessory rights,
2. investigate *search* and investigate *seizure*,
3. investigate existing statutes and opinions regarding search and seizure in an on-line computer network, and
4. examine the concept of a *reasonable expectation of Privacy* in an on-line computer network.

The primary sources of data for this study were:

- Corpus Juris Secundum,
- American Jurisprudence 2d,
- Lexis/Nexis

These legal resources contain state legal reporters, regional legal reporters, Supreme Court reporters, and numerous law journals.

The author also researched:

- relevant government documents,
- testimony before Congress and other agencies.

---

[126] Mitchell Kapor, and Michael Godwin. (1994). Civil liberties implications of computer searches and seizures: Some proposed guidelines for magistrates who issue search warrants [On-line]. Available as of July 1, 1996: http://www.eff.org/pub/Publications/Mike_Godwin /search_and_seizure_guidelines.eff.

The on-line resources of a number of other organizations were also interrogated for appropriate material. These sites included:

- the Electronic Frontier Foundation (EFF),
- the American Civil Liberties Union (ACLU),
- the Computer Professionals for Social Responsibility (CPSR),
- ERIC (Educational Resources Information Center), and,
- DIALOG (Dissertation Abstracts On-line).

This study provides a primer into principles of privacy and of search and seizure (and due process) that apply to AUPs by addressing the question: "How do privacy aspects of the First and Fourth Amendments impact the formulation of Acceptable Use Policy for an on-line computer network?" It is also important to explore the ways in which the answers to this question will be articulated in a university AUP.

CHAPTER IV

THE RESEARCH

> Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society ... now the right to life has come to mean the right to enjoy life—and right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession—intangible, as well as tangible.[127]

Introduction

Chapter II presented the views and opinions of scholars, law reviews, and special interest/advocacy groups. This chapter will present the ministrations of the judiciary and the Congress which may apply to Acceptable Use Policies and/or address the positions put forth in Chapter II. As a number of the issues are still being debated, this chapter will also attempt to provide a measure of objectivity to the various positions on the issues.

An Overview

The rapid advance and wide acceptance of computers and computer networks has spawned many contentious issues. The essential conflicts are between the individual user and the system's administration, and between the individual user and various law enforcement agencies. Universities and government agencies have acted to establish law to address the number of situations created by computer networks. These efforts might consist of some kind of vaguely stated policy which would then be enforced on a case-by-case basis.

---

[127] Samuel D. Warren and Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 193 (1890).

> The needs of society change with the increased use of and progress in technology. With the invention of the telephone and computer, communication has reached a new height in celebrity. Given enough resources and money, time no longer factors in as a constraint in gathering and distributing information. Along with the increase in the speed of communicating, the efficiency and ease of obtaining information also have increased. The tendency towards an information based society raises new issues that need to be resolved. One of those issues, privacy rights, demands our attention and resolution.[128]

As shown in a previous chapter, there has been a dramatic increase in the U.S. public's concern with privacy.[129] "In spite of the growing concern, response by the Congress has been lackluster."[130]

The American concern with the right to privacy appears to stem from efforts to define acceptable limitation on the amount of information concerning another which a person can acquire and distribute.[131] It appears that this is a sound assumption upon which to base the concern for the loss of privacy. The reasons for this rapid growth in a concern for privacy may include the revelations of the Watergate Hearings, or any number of other events. However, the vehicle for these events has been, and continues to be, *technology*. "With swift changes in technology, the public can no longer take privacy for granted."[132] Because less constraint on obtaining information about an individual by advancing telecommunication

---

[128] Right to privacy in the age of telecommunication [On-line]. (1996, March 26). Available as of July 1, 1996: http://www.tscm.com/full-text.html.

[129] See Figure 3, and U.S. Congress, Office of Technology Assessment. (1986). Federal government information technology: Electronic record systems and individual privacy. (Office of Technology Publication No. OTA-CIT-296). Washington, DC: U.S. Government Printing Office. page 26-27.

[130] Right to privacy in the age of telecommunication [On-line].

[131] Right to privacy in the age of telecommunication [On-line].

[132] Right to privacy in the age of telecommunication [On-line].

technology diminishes the degree of privacy an individual may enjoy, advancements in telecommunications provoke fear from the public. Therefore, with progressive technology, an explicit right to privacy should be defined and widely disseminated so that the public can understand what the 'ground rules' are and act accordingly.

> Unlike other constitutional rights where the courts interpreted explicitly defined rights, the right to privacy struggled to attain the status of a constitutional right because the courts and legislature defined and shaped the right to privacy according to the public's reactions to changes in the society. As can be seen through the rise of cases from Roberson v. Rochester Folding Box Company to Roe v. Wade, the court grappled with the problem of being in the position of defining what has been an implicit right explicitly. The fact that legislative actions have been reactive instead of progressive compounded the difficulty of anchoring any lucid privacy rights firmly into our society. Detailed examination of some of the privacy invasion issues in rapidly changing telecommunication technology will demonstrate that the right to privacy cannot continue to be defined by capricious approach.[133]

The Role of Privacy in Our Lives

> Let there be space in your togetherness.[134]

Privacy was not given to us in the same manner that our common law was - it did not come from England.[135] Frequently referred to as, "The American Tort," privacy was born in a law review article by Louis Brandeis and John Warren, published in 1890,[136] which advocated that we should adjust our customs, metaphors and rules to account for that which can intrude on our basic right "to be let alone."[137]

---

[133] Right to privacy in the age of telecommunication [On-line].

[134] Kahlil Gibran. (1923). The prophet. New York: Phoenix Press.

[135] Seipp, English Judicial Recognition of a Right to Privacy, 3 Oxford J. Leg. Stud. 325 (1983).

[136] Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harvard L. Rev. 193 (1890).

[137] Samuel Warren and Louis Brandeis, The Right to Privacy at 195.

Modern technology has accentuated existing problems, and created other concerns regarding privacy. Computer use has resulted in tremendous improvements in the processing and accessibility of information, which was always available, but which was previously protected by *logistical barriers*. One had to be physically where the information was stored to access it. Today, such personal information as credit records, bank records, insurance information, and criminal data are readily available from both governmental and private sources, and physical presence at the site of storage is no longer required.[138]

> Accordingly, issues of informational privacy arise with increasing frequency, and the capabilities of the technology present new challenges in balancing the utility of sharing personal information against the value of individual privacy. As more information becomes available, a natural conflict develops between those who want access to information and those who want to protect it. Each of us wants information about others, but we desire to keep private the information about ourselves, except where it suits our purpose to disclose portions of it. The power to limit the availability of personal information may be the heart of privacy, although surely it frustrates public curiosity.[139]

Roots of the Term *Privacy*

> Privacy, like an elephant, is more readily recognized than described.[140]

The British scholar Raymond Williams has traced the root of the term *privacy* to the Latin word *privatus*, which means to withdraw from public life, and/or to have seclusion from the public.[141]

---

[138] U.S. Congress, Office of Technology Assessment. (1986). Federal government information technology: Electronic record systems and individual privacy. (Office of Technology Publication No. OTA-CIT-296). Washington, DC: U.S. Government Printing Office.

[139] Justice Society (Committee on Privacy). (1983). Privacy and the law. London: Fontana Paperbacks.

[140] Young, John B. (1978). Privacy. New York: John Wiley & Sons.

[141] Raymond Williams. (1976). Keywords: A vocabulary of culture and society. London: Fontana Press, page 203.

The modern day "Right of Privacy" is a "generic term encompassing various rights recognized … to be 'inherent in the concept of ordered liberty'…including protection from governmental indifference."[142] This right is not an absolute one, and does not apply to conduct that may be harmful to other individuals or to society.

Privacy in Our Public Society

> The so-called right of privacy is, as the phrase suggests, founded upon the claim that a man has the right to pass through this world, if he wills, without having his business enterprises discussed, his successful experiments written up for the benefit of others, or his eccentricities commented upon either in handbills, circulars, catalogues, periodicals or newspapers.[143]

In Paradise Lost,[144] John Milton discussed the concept of privacy but went beyond the personal aspects. "Paradise Lost is about the loss of Eden, the loss of

---

[142] The *Right of Privacy* is a general right to be left alone. Katz v. United States, 389 U.S. 347 (1967). The *Right of Privacy* is a "generic term encompassing various rights recognized . . . to be 'inherent in the concept of ordered liberty' … including protection from governmental indifference." Industrial Foundation of the South v. Texas Industrial Accident Board, 540 S.W.2d 668, 679 (1976). The four forms of invasion of privacy are unreasonable intrusion upon seclusion, appropriation of name or likeness, unreasonable publicity given to a person's private life, and placing another in false light before the public." 77 C.J.S. Right to Privacy and Publicity 488. Privacy is also a right to "live life free from unwarranted publicity." Harms v. Miami Daily News, 127 So.2d 715, 716 (1961). Although the term *privacy* is not mentioned in the US Constitution, it has been defined by the Supreme Court, through the years, in a line of decisions. The Court has held in: Griswold v. Connecticut, 381 U.S. 479 (1965) ([S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create 'zones of privacy'. The right of association contained in the penumbra of the First Amendment is one …); See also, Roe v. Wade, 410 U.S. 113 (1972) (The Constitution does not explicitly mention any right of privacy. In a line of decisions, however, … the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution. This right of privacy … is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.).

[143] Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 544 (1902) (The court found that the theory was too broad to be enforced and suggested that the legislature could enact statutes so that "the rule would be applicable only to cases provided for by the statute." In response, the New York legislative body enacted Section 50 and 51 of New York Civil Rights Law recognizing the right of privacy.)

[144] John Milton. (1987). Paradise lost New York: Chelsea House, p156.

innocence, and the loss of privacy."[145] Arnold Stein's reflection of Milton's epic message is important as it provides insight into 'private life':

> Related (to the known cultural history of *Gan Eden*) is the occasional human yearning for peace and quiet, for an impossibly ideal Arcadia where wilderness may be thought paradise snow; or there is the desire to withdraw from complexity, from 'the fury and mire of human veins, 'to withdraw even, especially, from the self and its involvement's ...[146]

Hixson notes that "the terrible irony in man's ageless search for solitude and seclusion, the paradise that is inevitably lost and the privacy that is so temporary [is] nearly always invaded."[147] And little did the inhabitants of the *Garden of Eden* realize that their privacy and solitude would be invaded, first by Satan, and then by the Archangel Michael, who, (in the final scene of Paradise Lost) instructs them to leave. Milton's account of the first experience with the loss of privacy thus concludes:

> The World was all before them, where to choose
> Their place of rest, and Providence their guide:
> They went hand in hand with wandering steps and slow,
> Through Eden took their solitary way.[148]

Many early civilizations have been characterized by the place and meaning of privacy in their culture. Without delving into the specific beliefs of various ancient cultures in regard to privacy, it can be noted that there was an antithetical posture between the need for privacy and the desire for public authority.

The quotation below from Genesis shows that there was no desire on anyone's part to intrude.

> And Noah began to be a husbandman, and planted a vineyard: and he drank of the wine, and was drunken; and he was uncovered within his tent. And Ham, the father of Canaan, saw the nakedness of his father, and told his two brethren without. And Shem and Japheth took a garment, and laid it upon both their

---

[145] Richard F. Hixson. (1987). Privacy in a public society. New York: Oxford Univ. Press. page. 4.

[146] Arnold Stein. (1952). Answerable style: Essays on paradise lost. Minneapolis: Univ. of Minnesota, page 4.

[147] Richard F. Hixson. (1987). Privacy in a public society. New York: Oxford Univ. Press. page. 4.

[148] John Milton. (1987). Paradise lost. New York: Chelsea House, page 122.

> shoulders, and went backward, and covered the nakedness of their father; and their faces were backward, and they saw not their father's nakedness.[149]

We are also told that there *was* a sense of intrusion on the part of the sons, but they instinctively withdrew in order not to infringe upon their father's privacy.

The theme of privacy runs historically through the Bible. It illustrates an understanding of personal privacy and the conflict between our need to depend upon other people and our desire for seclusion. This theme of "privacy as a right against authority"[150] is noted throughout history. It has also been shown to have been an integral part of early Hebrew, classical Greek, and ancient Chinese culture. Barrington Moore, Jr., notes that, "... man has to live in society, and social concerns have to take precedence."[151] In Moore's view, these initial attempts of many civilizations to separate and balance the concepts of personal privacy and public authority continue throughout the ages.

In the Middle Ages, privacy interests were virtually non-existent. Power struggles among churchmen and monarchies were prevalent; thus, the rights of an individual were not honored. Moore indicates that it was not until a less parochial bourgeoisie generated a new belief in the notion of privacy that people began to be aware of what 'privacy' meant and what it did not mean.[152] But it was not until the latter part of the nineteenth century that privacy began to be accepted in legal terms.

The ancient concepts of solitude are evident in early America. Privacy there was not one of the dominant concerns; however, it was an issue. The Puritan settlements were based upon a belief in community which obligated the citizens to

---

[149] Frank Allen Patterson. (1933). The student's Milton. New York: Columbia Univ. Press. page 646.

[150] Richard F. Hixson. (1987). Privacy in a public society. New York: Oxford Univ. Press. page 4.

[151] Barrington Moore, Jr. (1984). Privacy: Studies in social and cultural history. New York: Random House. page 267-277.

[152] Barrington Moore, Jr. (1984). Privacy: Studies in social and cultural history. New York: Random House.

band together for protection and mutual encouragement. Flaherty states that in Puritan America, "... privacy took second place to other values in the location of homes until Puritan communitarian ideals gradually disintegrated in the face of New World conditions."[153] Privacy is not mentioned in the Constitution, but the Fourth Amendment, *de facto*, forbids some invasions of it. Privacy may not be explicitly defined (in the Constitution), but its aura is often noted.[154]

Flaherty additionally notes that "the ordinary colonial family could enjoy intimacy, as well as an almost automatic degree of solitude."[155] It was much easier in colonial days to remove oneself from the 'public scene.' Today, there are few reclusive refuges available. As the early colonists became less and less dependent upon a communal style of living they began to physically spread out and become more diverse in their needs and desires.

Hixson notes that the:

> colonial household between 1700 and 1740 was necessarily a rather basic enterprise, even in the growing seaport towns, with no running water, only passable lighting, no refrigeration or screening, and minimal privacy. The desire for privacy in daily life then, as now, was also a by product of a person's work and the work place environment.[156]

Flaherty observes that:

> Although colonial New England was in general a democratic society . . . the concept of deference, which pervaded all aspects of life, modified any elements of antipathy to privacy implicit in the notion of democracy. This was unlike the situation in late-nineteenth-century America when a popular interpretation of the meaning of democracy sometimes associated a conscious search for privacy with aristocratic tendencies. The colonial sense of deference stimulated a respect for other persons, particularly one's betters and for their privacy.[157]

---

[153] David H. Flaherty. (1972). Privacy in colonial New England. Charlottesville, VA: Univ. of Virginia, page 72.

[154] Industrial Foundation v. Texas Industrial Accident Board, 540 S.W.2d 668, 679 (1976).

[155] David H. Flaherty. (1972). Privacy in colonial New England. Charlottesville, VA: Univ. of Virginia, page 30.

[156] Richard F. Hixson. (1987). Privacy in a public society. New York: Oxford Univ. Press, page 9.

[157] David H. Flaherty. (1972). Privacy in colonial New England. Charlottesville, VA: Univ. of Virginia.

It was not until the latter Nineteenth Century that legal thinkers began to conceive of the notion of privacy as a legal right. Warren and Brandeis credited Judge Thomas Cooley, who, in his famous treatise on torts published in 1879, spoke of the right "to be let alone" [158] as matter of personal security. In a very interesting side note, Yale Law School librarian, Fred R. Shaprio[159] states that Warren and Brandeis' article was the most cited pre-1947 law review article. Shapiro's statement is based upon data from the Institute for Scientific Information's database.

Warren and Brandeis note that:

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' The press is overstepping in every direction the obvious bounds of property and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle.[160]

New developments in technology and business methods require that the next step be taken to protect our right "to be let alone."[161] Just as Warren and Brandeis advocated in their 1890 law journal article, we should adjust our metaphors, customs, and rules to account for that which can intrude on our basic *right to be let alone* and not intruded upon. Warren's and Brandeis's argument was that, while some aspects of privacy involve the ownership or possession of real property, we need to protect human 'personality.'[162] They wanted to extend the scope of the law to include a

---

[158] Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harvard L. Rev. 195 (1890).

[159] Fred R. Shaprio. (1987). The most cited law review articles. Buffalo, NY: W. Hein Co.

[160] Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harvard L. Rev. 193 (1890).

[161] Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harvard L. Rev. 193 (1890).

[162] Warren and Brandeis at 202.

person's feelings and emotions.[163] Warren's and Brandeis's law review article synthesized a whole new category of legal rights and initiated a new field of jurisprudence.

This notion of privacy which Warren and Brandeis put forth was supported by a number of legal thinkers of the time. However, Judge Denis O'Brien was a bit skeptical when he stated in 1902 in the Columbia Law Review that:

> The right of privacy in such cases, if it exists at all, is something that can not be regulated by law. The rules for the regulation of human conduct with respect to the courtesies and proprieties of life and that enjoin that delicate regard for the feelings and sensibilities of others are not to be found in statutes or judicial decisions.
>
> The moment one voluntarily places himself before the public, either in accepting public office, or in becoming a candidate for office, or as an artist or literary man, he surrenders his right to privacy, and obviously cannot complain of any fair or reasonable description or portraiture of himself.[164]

Court decisions over the last 100 years, however, have ruled that if people do not become part of the public then they are entitled to their solitude--their privacy, and that privacy cannot be easily or frivolously taken away.

In 1928, the Supreme Court ruled that a person's privacy was not invaded via the wiretap since there was no actual (physical) entry into the house in question. Louis Brandeis took the government to task for allowing wiretap evidence to be gathered via a telephone and then used as evidence against a person. Brandeis stated that:

> To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.[165]

---

[163] See generally, Warren and Brandeis. The Right to Privacy, 4 Harvard L. Rev. 193 (1890).

[164] Denis O'Brien, __ Columbia L.Rev __ (1902).

[165] Olmstead v. United States, 277 U.S. 438 (1928).

The law of the land in 1928 did not yet recognize that the right to privacy included a person's character. It was not until early 1967 that the common law right to privacy yielded to the Supreme Court's intervention in this area in Katz v. United States.[166] The Supreme Court spoke to a *constitutional right of privacy* which protected citizens from governmental officials. Over the years this right was expanded to:

> protect the autonomy of the individual to make certain important decisions of a very personal nature in such matters as marriage, procreation, contraception, family relationships, child rearing, and education.[167]

In their search for solitude (privacy), Americans invented barbed wire, and proceeded to build fences on the frontier throughout the mid to late 1800s. The private Pullman compartment was invented when railroads became the rage. In the United States, even the cheapest hotel often has a private bathroom for each of its rooms. Such is not the case in most other parts of the world. In more recent times, the suburb came into being when Americans felt a need for more privacy - city life was too public. Americans have a deep-rooted concern for privacy, and have always sought to satisfy their desire to "be let alone."[168]

---

[166] Katz v. United States, 389 U.S. 347 (1967). Defendant Katz was, convicted in the United States District Court for the Southern District of California, of a violation of statute proscribing interstate transmission of wire communication of bets or wagers, and he appealed. The Court of Appeals, 369 F.2d 130, affirmed, and certiorari was granted. The Supreme Court held that government's activities in electronically listening to and recording the defendant Katz's words spoken into telephone receiver in public telephone booth violated the privacy upon which the defendant justifiably relied while using the telephone booth. Thus this action constituted a "search and seizure" within Fourth Amendment, and the fact that electronic device employed to achieve that end did not happen to penetrate the wall of the booth could have no constitutional significance. The Court further held that the search and seizure, without prior judicial sanction and attendant safeguards, did not comply with constitutional standards. Although, accepting the account of the government's actions as accurate, the magistrate could constitutionally have authorized with appropriate safeguards the very limited search and seizure.

[167] 16A Am. Jur. 2d, Constitutional Law, §§601-606.

[168] Warren and Brandeis at 195.

Privacy in General

In a law review article, Dean Prosser classified the privacy tort into ". . . four separate causes of action,"[169] or forms of invasion of privacy. As a result of Prosser's article, and, as a result of his being the drafter of the Restatement (Second) of Torts, these classifications have been recognized in a large number of court decisions.[170]

These categories of invasion have been described as "distinct wrongs,"[171] and as, "loosely related but distinct"[172] causes of action. The forms are:

- an unreasonable intrusion upon seclusion,[173]
- appropriation of a person's name and/or likeness for commercial use/benefit,[174]
- unreasonable publicity given to a person's private life,[175] and,
- placing a person in a false light before the public.[176]

---

[169] Dean Prosser, Privacy, 48 Cal. L. Rev. 383 (1960); 62A Am. Jur. 2d Privacy 665.

[170] Factors Ect. v. Pro Arts, 579 F.2d 215 (1978), 4 Media L.Rev. 1144, 205 USPQ 751, cert den 440 U.S. 908, 59 L.Ed.2d 455, 99 S.Ct. 1215 and on remand 496 F.Supp 1090, 208 USPQ 529, rev 652 F.2d 278, 7 Media L.Rev. 1617, 211 USPQ 1, cert den 456 U.S. 927, 72 L.Ed.2d 442, 102 S.Ct. 1973, and on remand 541 F.Supp 231, 8 Media L.Rev. 1839, vacated 562 F.Supp. 304, 9 Media L.Rev. 1642 and reh den 701 F.2d 11, 9 Media L.Rev. 1110 and (disagreed with by Rogers v. Grimaldi (CA2 NY) 875 F.2d 994, 16 Media L.Rev. 1648, 10 USPQ2d 1825); Cummings v. Walsh Constr. (SD Ga.) 561 F.Supp 872, 31 BNA FEP Cas 930, 115 BNA LRRM 4070; Pierson v. News Group Publications, (SD Ga.) 549 F.Supp 635; Beard v. Akzona, 517 F.Supp 128; Fogel v. Forbes, 500 F.Supp 1081, 6 Media L.Rev. 1941 (applying Pennsylvania law).

[171] Phillips v. Smalley Maintenance, 435 So.2d 705 (1983).

[172] Sun v. Langston, 316 S.E.2d 172, 170 Ga.App. 60 (1984).

[173] Sun v. Langston, 316 S.E.2d 172, 170 Ga.App. 60 (1984).

[174] McCall v. Courier-Journal and Louisville Times, 623 S.W.2d 882, cert den 102 S.Ct. 2239, 456 U.S. 975; 72 L.Ed.2d 849; Struner v. Dispatch Printing, 442 N.E.2d 129, 2 Ohio App.3d 377, 2 O.B.R. 435; Covington v. Houston Post, 743 S.W.2d 345; Restatement (Second) of Torts, §625A(2)(b), §68.

[175] McCall v. Courier-Journal and Louisville Times, 623 S.W.2d 882, cert den 102 S.Ct. 2239, 456 U.S. 975; 72 L.Ed.2d 849; Struner v. Dispatch Printing, 442 N.E.2d 129, 2 Ohio App.3d 377, 2 O.B.R. 435; Covington v. Houston Post, 743 S.W.2d 345; Restatement (Second) of Torts, §625A(2)(b), §68.

[176] Cantrell v. Forest City Pub., 95 S.Ct. 465 (1974), 419 U.S. 245, 42 L.Ed.2d 419; Hogin v. Cottingham, 533 So.2d 525; Goodrich v. Waterbury Republican-American, 448 A.2d 1317, 188 Conn. 107; Restatement (Second) of Torts, §625A(2)(d), §120 et. seq.

In this dissertation, attention will be focused exclusively on 'intrusion upon seclusion' as it is not likely that the other three elements will impact the unique situations which will confront the framers of Acceptable Use Policies.

A linchpin concern at this juncture seems to be to attempt to establish what the scope and limits of 'privacy' are in an AUP. To do so will define the custom which will establish precedent as to what is legal and acceptable for an administration to *do* and/or *not to do* in regard to a user's account. There is no legal cause for action based upon an invasion of privacy for matters which occur in a public place or in a place which is otherwise open to the public.[177]

An individual's right to privacy is not necessarily superior to the rights of the public.[178] In determining the scope and limits of a person's right to privacy, it is important to consider the rights and responsibilities of a person as a citizen of a free country.[179] It is equally important to view an individual's right to privacy as it relates to the community in which that person is a member.[180] A "conflict between the public's right to information and an individual's right to privacy requires a balancing of competing interests ... In balancing these interests there are occasions in which the public right must prevail."[181]

A tactic to negate liability under an invasion of privacy action may be to have all university computer users sign a waiver of their rights to privacy. However Mike Godwin, the Electronic Frontier Foundation's legal counsel, states that to consider

---

[177] 77 C.J.S. Right to Privacy and Publicity 482; Hartman v. Meredith Corp., 638 F.Supp. 1015 (1986).

[178] 77 C.J.S. Right to Privacy and Publicity 485; Mavity v. Tyndall, 66 N.E.2d 755 (1946), 224 Ind. 364, appeal after remand 74 N.E.2d 914, 225 Ind. 360, appeal dismissed Indiana on relation of Mavity v. Tyndall, 68 S.Ct. 609, 333 U.S. 834, 92 L.Ed. 1118, reh den 68 S.Ct. 732, 333 U.S. 858, 92 L.Ed 1138.

[179] Barber v. Time, Inc., 159 S.W.2d 291, 348 Mo. 1199.

[180] McGovern v. Van Riper, 54 A.2d 469, 140 N.J.Eq. 341.

[181] 77 C.J.S. Right to Privacy and Publicity 486; Vassiliades v. Garfinckel, Brooks Bros., App., 492 A.2d 580 (date).

such a global waiver as policy would be "transcendentally stupid ... on the part of a [system administrator, as] it eliminates ... [the] ability to claim [Electronic Community Privacy Act] protections if ... e-mail is wrongfully seized. And it eliminates the ability of [the] users to file a class action suit against the government."[182]

As one delves further into the scope and limits of privacy, it becomes doubtful that the right to privacy is an inherent right of a user of a university's computer system. Aside from the mandates of the Electronic Communications Privacy Act (ECPA), the Privacy Act of 1974, and the Family Educational Records Privacy Act (FERPA), the legal concept of privacy (the right to privacy) appears to be a condition that can be determined by local authority. Thus, it seems appropriate that the university can define what a computer user's expectations of privacy are through its Acceptable Use Policy (AUP).

Seminal Statutes/Cases Applicable to Privacy

> Our cases long have recognized that the Constitution embodies a promise that a certain private sphere of individual liberty will be kept largely beyond the reach of government.[183]

Louis D. Brandeis was appointed by President Wilson as an Associate Justice of the Supreme Court in 1916, and served until his retirement in 1939. Judge Brandeis was viewed as representing those who lobbied for new concepts in social legislation. He was replaced by William O. Douglas, who served until his retirement in 1975.

Although a replacement justice generally does not hold a philosophy similar to that of the justice he replaces, these two men held amazingly similar points of view. In

---

[182] Michael Godwin. (1994, May 10). Logon disclaimers waiving the ECPA. Posted to: alt.bbs newsgroup.

[183] Thornburgh v. American College of Obstetricians & Gynecologists, 476 U.S. 747, 772 (1986) (Harry A. Blackmun, J.).

a quite pragmatic sense, Brandeis, and then Douglas, occupied what was known as the "*privacy seat*" on the Court for over half a century.

It was not until 1928 that Brandeis had an opportunity to present a case for constitutional privacy. His vehicle for doing so was Olmstead v. United States,[184] a case which dealt with the Fourth Amendment prohibition in regard to "unreasonable searches and seizures."[185]

The Fourth Amendment

> The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home—a zone that finds its roots in clear and specific constitutional terms: "the right of the people to be secure in their … house … shall not be violated.[186]

The Fourth Amendment states that people have the right to be "secure in their persons, houses, papers and effects against unreasonable searches and seizures,"[187] But it does not go on to define "unreasonable."[188] The interpretation here has been left to the U.S. Supreme Court.

There are two possible interpretations of the Fourth Amendment. One view of the Amendment is that it means exactly what is says. It does not protect fields, or phone lines, or anything other than "persons, houses, papers and effects."[189] Based upon this position it is not reasonable to search "persons, houses, papers and effects"[190] absent a search warrant being issued.

Another view is that this amendment was intended to generally protect the right of private property against government trespass. This point of view

---

[184] Olmstead v. United States, 277 U.S. 438 (1928).
[185] U.S. Const. amend IV.
[186] Payton v. New York, 445 U.S. 573, 589 (1980) (John Paul Stevens, J.).
[187] U.S. Const. amend IV.
[188] U.S. Const. amend IV.
[189] U.S. Const. amend IV.
[190] U.S. Const. amend IV.

encompasses the notion that technological developments should extend the concept and right of privacy to those 'developments.' But it should do so, not based upon accidents of technology, but upon the interpretation of the fundamental principles of the Constitution.

During the first half of the twentieth century, a majority of the U.S. Supreme Court held a combination of these two views.

Olmstead v. United States[191]

Olmstead involved an FBI wiretap of Olmstead and seventy other people who were engaged in a conspiracy to transport and sell liquors in violation of the Eighteenth Amendment[192] (National Prohibition Act of 1919). Evidence of the conspiracy was obtained by the use of wiretaps. The Court ruled that the wiretaps were made without having to physically trespass on private property because the phone wires were not part of Olmstead's house or office. The Court found that the Fourth Amendment had not been violated as there had been no physical invasion. Brandeis noted in his dissent of Olmstead:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed must be deemed a violation of the Fourth Amendment.[193]

---

[191] Olmstead v. United States, 277 U.S. 438 (1928).

[192] U.S. Const. amend. XVIII. "One year from ratification of this article the manufacture, sale, or transportation of intoxicating liquors within, importation thereof into, or exportation thereof from the United States and all its territory subject to the jurisdiction thereof for beverage purpose is hereby prohibited."

[193] Olmstead at 478.

In this dissenting opinion, Justice Brandeis argued that Olmstead's rights had still been violated, even though "persons, houses, papers and effects"[194] had not physically been searched or trespassed upon. He argued that the question at hand was whether Olmstead's inherent right to privacy had been violated, and not that his property was (or was not) physically trespassed upon. Brandeis's position was that there is a critical difference between the right one has in regard to personal property and the right one has to privacy.

Griswold v. Connecticut[195]

> In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion.[196]

A Connecticut statute made it a crime to use "any drug, medicinal article or instrument"[197] for the purpose of birth control. Another statute in Connecticut made it a crime to aid a person in the act of birth control. In Griswold, the executive director and the medical director of the Planned Parenthood League of Connecticut were convicted under these statutes as they provided birth control devices and other material to married couples.

The Supreme Court reversed the lower court's ruling, and established a landmark philosophy regarding the right to privacy.

---

[194] Olmstead at 479.

[195] Griswold v. Connecticut, 381 U.S. 479 (1965). The defendants were convicted of violating Connecticut's birth control law. The Circuit Court of the Sixth Circuit, Connecticut, rendered judgments against the defendants, and the defendants appealed. The Appellate Division of the Circuit affirmed the lower court's decision, and the defendants appealed. The Connecticut Supreme Court of Errors, 151 Conn. 544, 200 A.2d 479, affirmed the lower court's decision, and the defendants appealed. The U.S. Supreme Court reversed the Connecticut courts. The Supreme Court held that the Connecticut law forbidding the use of contraceptives unconstitutionally intrudes upon the right of marital privacy.

[196] Griswold at 483.

[197] Griswold at 480.

The aforementioned cases lead the Supreme Court to state that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance ... Various guarantees create zones of privacy."[198]

Katz v. United States[199]

In 1967 the Supreme Court overruled the Olmstead[200] decision of 1928. The Court essentially rejected the Olmstead notion that there needed to be a "physical intrusion . . . [or] trespass"[201] into a given area before there can be an invasion of one's privacy. Katz clearly established that the Fourth Amendment "protects people" and not places.

Cubby v. Compuserve[202]

> "NEW YORK, NEW YORK, USA, 1991 OCT. 31 (NB)--U.S. District Judge Peter Leisure ruled that CompuServe cannot be held liable for information in a newsletter it did not originally publish. His decision, the first of its kind, held that computer databases are the equivalent of newsstands or book stores, whose owners cannot be held liable for the content of the papers they sell unless they know beforehand that the stories are false."

---

[198] Griswold at 482.

[199] Katz v. United States, 389 U.S. 347 (1967). Defendant Katz was, convicted in the United States District Court for the Southern District of California, of a violation of statute proscribing interstate transmission of wire communication of bets or wagers, and he appealed. The Court of Appeals, 369 F.2d 130, affirmed, and certiorari was granted. The Supreme Court held that government's activities in electronically listening to and recording the defendant Katz's words spoken into telephone receiver in public telephone booth violated the privacy upon which the defendant justifiably relied while using the telephone booth. Thus this action constituted a "search and seizure" within Fourth Amendment, and the fact that electronic device employed to achieve that end did not happen to penetrate the wall of the booth could have no constitutional significance. The Court further held that the search and seizure, without prior judicial sanction and attendant safeguards, did not comply with constitutional standards. Although, accepting the account of the government's actions as accurate, the magistrate could constitutionally have authorized with appropriate safeguards the very limited search and seizure.

[200] Olmstead v. United States, 277 U.S. 438 (1928).

[201] Olmstead at 484.

[202] Cubby v. Compuserve, 766 F.Supp 135 (1991).

In Cubby, the defendant CompuServe was an on-line service providing subscribers with access to a variety of special interest databases and forums. The *Journalism Forum* carried false and defamatory statements about the plaintiffs who were developers of an electronic news and gossip magazine entitled "Skuttlebut."[203] "CompuServe did not dispute that the statements concerning the plaintiff were defamatory."[204] Rather, CompuServe argued that it "acted as a distributor, and not a publisher, of the statements, and cannot be held liable for the statements because it did not know and had no reason to know of the statements."[205]

"CompuServe had no opportunity to review the contents of publications before they were uploaded into the company's computer data banks. Conversely, the plaintiffs argued that CompuServe was a *publisher* of the false statements and should be held to the higher standard of liability accompanying such designation."[206]

At issue was the standard of liability which should be imposed upon CompuServe. If CompuServe could be likened to an electronic library or bookstore, then it would be considered a distributor of published material.[207] In Smith v. California,[208] the Supreme Court held that a distributor must have knowledge of the contents of a publication before imposing liability for its distribution. In Smith, the Court struck down an ordinance which imposed liability on a bookseller for possession of an obscene book irrespective of whether the bookseller actually had knowledge of the book's contents.[209] The Court observed that "[e]very bookseller would be placed under an obligation to make himself aware of the contents of every

---

[203] Cubby at 138.

[204] Marc L. Caden and Stephanie E. Lucas, Comment, Accidents on the Information Superhighway: On-Line Liability and Regulation, 2 Rich. J.L. & Tech. 3 (1996). Available as of July 1, 1996: http://www.urich.edu./~jolt /v2i1/caden_lucas.html.

[205] Cubby at 137.

[206] Caden and Lucas at para. 18.

[207] See generally, Caden and Lucas.

[208] Smith v. California, 361 U.S. 147 (1959).

[209] Smith at 155.

book in his shop. It would be altogether unreasonable to demand so near an approach to omniscience."[210] Thus, "a distributor is a passive receptacle for information and will not be held liable in absence of actual knowledge."[211]

"If CompuServe was found to have *published* the defamatory statement, it would have been liable as a culpable party because a publisher who republishes or repeats a defamatory statement is subject to the same liability as if it had originally published the statement."[212] Whether or not a party is characterized as a publisher is largely dependent upon the degree of editorial control that is exercised over the given publication. For example, "a newspaper exercises a high degree of control over its final product with respect to editorial judgments and ultimate content."[213] In Miami Herald Publishing Co. v. Tornillo,[214] the Court held that the "choice of material to go into a newspaper, and the decisions made as to limitations on the size and content of the paper and treatment of public officials ...constitute the exercise of editorial control and judgment."[215] Thus, "newspapers are considered publishers within the legal context of libel and defamatory statements."[216]

The court characterized CompuServe's product as an "electronic, for-profit library"[217] which provides a variety of publications and collects subscriber fees in return for access. More importantly, the court found that "CompuServe has no more control over such a publication than does a public library, book store, or newsstand,

---

[210] Smith at 153 (quoting The King v. Ewart, 25 N.Z.L.R. 709, 725 (1905).

[211] Caden and Lucas at para. 19.

[212] Caden and Lucas at para. 20. See also, Hoover v. Peerless Publications, 461 F.Supp. 1206, 1209 (1978) (noting that one who republishes libel is subject to the same liability as if he had originally published such a statement, even if the republisher attributes the libelous statements to the original publisher); Restatement (Second) of Torts, §578 (1976) ("one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it.").

[213] Caden and Lucas at para. 20.

[214] Miami Herald Publishing v. Tornillo, 418 U.S. 241 (1974).

[215] Miami Herald at 258.

[216] Caden and Lucas at para. 20.

[217] Cubby v. Compuserve, 776 F.Supp. 135, 140 (1991).

and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so."[218] Therefore, the court granted summary judgment in favor of CompuServe.[219]

By labeling CompuServe as a distributor rather than a publisher, the court issued the first prominent legal decision concerning the culpability of on-line access providers. The decision encouraged growth within the Internet community by reducing the threat of liability to on-line access providers.[220]

So, although we often talk about BBSs as having the rights of publishers and publications, this accentuates an important distinction. How are publishers different from bookstore owners? Because we expect a publisher (or its agents) to review everything prior to publication. But we do not expect bookstore owners to review everything prior to sale. Similarly, in the CompuServe case, as in any case involving an on-line service in which users freely post messages for the public, we would not expect the on-line communications service provider to read everything posted before allowing it to appear.

It is worth noting that the Supreme Court case on which Judge Leisure relies is Smith v. California,[221] an obscenity case, not a defamation case. Smith is the Supreme Court case in which the notion first appears that it is generally unconstitutional to hold bookstore owners liable for content. So, if Smith v. California applies in a on-line-service or BBS defamation case, it certainly ought to apply in an obscenity case as well.

---

[218] Cubby at 140.
[219] Cubby at 141.
[220] Caden and Lucas at para 22.
[221] Smith v. California, 361 U.S. 147 (1959).

Thus, CompuServe sheds light not only on defamation law as applied in this new medium but on obscenity law as well. This decision should do much to clarify to concerned sysops (system operator) what their obligations and liabilities are under the law.

Stratton Oakmont v. Prodigy[222]

On May 26, 1995 the New York Times reported that:

> In a ruling that could change the nature of on-line information services, a New York judge cleared the way Thursday for a $200 million libel lawsuit against the Prodigy Services Company when he ruled that the popular on-line network was a publisher of information, not just a distributor.

And, according to a Reuters news release on May 26, 1995, "The ruling is the first time a computer bulletin board has been held subject to a libel suit."[223] However other issues are involved, and the case will likely turn on those other issues.

On May 24, 1995, the Supreme Court of New York granted partial summary judgment against Prodigy Services Company, finding that it had exercised sufficient editorial control over its computer bulletin boards to incur liability as a publisher.[224] Prodigy subscribers are able to communicate with one another through various bulletin boards. One such bulletin board was *Money Talk*, a widely read financial bulletin board, where members could post statements concerning stocks, bonds, investments, and related financial matters. The plaintiffs, Stratton Oakmont, Inc., a securities investment banking firm, and its president, Daniel Porush, brought an action for *per se libel* for statements posted about them on Prodigy's *Money Talk* computer bulletin board in 1994. The posting reflected that Porush was soon to be proven

---

[222] Stratton Oakmont v. Prodigy, 1995 NY Misc. LEXIS 229.
[223] Stratton Oakmont.
[224] 23 Media L. Rep. (BNA) 1794, 1795 (N.Y. Sup. Ct. 1995).

criminal and that Stratton Oakmont, Inc., was a "cult of brokers who either lie for a living or get fired."[225]

The plaintiffs contended that Prodigy had held itself out as an on-line service which was family oriented. In an effort to provide a family environment, Prodigy edited the content of messages posted on its bulletin boards. Prodigy made no apology

> for pursuing a value system that reflects the culture of the millions of American families . . . [and] no responsible newspaper does less when it chooses the type of advertising it publishes.[226]

Stratton Oakmont further argued that statements such as the prior remark by a Prodigy official were tantamount to an admission which proved that Prodigy was akin to a newspaper. As such, Prodigy should incur liability for defamatory statements posted on its bulletin boards as a publisher.[227]

Prodigy openly advertised that all e-mail and postings are screened. They have stated that they delete anything that does not comply with their rules. Prodigy has also announced that it is a place where children would not be exposed to sex and other illegal activity. "And therein lies the hook by which Prodigy became a party to this lawsuit. By their statements, Prodigy assumed direct responsibility for the happenings on their system."[228] The judge in this case specifically said that the holdings in CompuServe did not apply to this case, as CompuServe Information Systems doesn't claim to edit content. Because Prodigy had made a prior policy of scanning for content, the judge held Prodigy to a different standard.

---

[225] Stratton Oakmont v. Prodigy, 1995 NY Misc. LEXIS 229.
[226] Stratton Oakmont (quoting Exhibit J).
[227] Stratton Oakmont at 1795-96.
[228] Caden and Lucas at para 26.

Implications from Cubby and Prodigy

Judge Ain, in writing the Prodigy opinion, observed "that Prodigy's current system . . . may have a chilling effect on freedom of communication in cyberspace, and it appears that this chilling effect is exactly what Prodigy wants, but for the legal liability that attaches to such censorship."[229] Judge Ain was not attempting to promote *chilling effect* by deciding against Prodigy. However, Prodigy may now serve as a vehicle to curtail or discourage the development of the Internet by causing access providers to fret about potential legal culpability.[230] "Worse yet, access providers may turn a blind eye to any and all communications disseminated through their services in an effort to reduce their potential liability as a publisher. This may result in an increase in Internet activity involving precisely the kind of material, such as pornography and bomb-making manuals, currently generating paranoia among the general public."[231]

Cubby was clearly an opinion which favored access providers as it severely reduced their level of culpability. Although it provided a different verdict, Prodigy agreed that access providers "should generally be regarded in the same context as bookstores, libraries, and network affiliates."[232] However, the Prodigy court found that it was Prodigy's own conscious decisions which altered its liability and resulted in it being labeled a publisher. "Prodigy's conscious choice to gain the benefits of editorial control has opened it up to greater liability than CompuServe and other networks that make no such choice."[233]

---

[229] Prodigy, 23 Media L.Rep. (BNA) at 1798.

[230] See generally, 23 Media L.Rep. 1794.

[231] Caden and Lucas at para 28.

[232] Prodigy, 23 Media L.Rep. (BNA) at 1798. See also, Edward V. DiLello, Functional Equivalency and Its Application to Freedom of Speech on Computer Bulletin Boards, 26 Colum. J.L. & Soc. Probs. 199, 210-211 (1993).

[233] Prodigy, 23 Media L.Rep. (BNA) 1798

It appears that lines of demarcation with respect to liability will ultimately be drawn by Congress. The court in Prodigy observed that the issues it considered may be preempted by federal law if the Communications Decency Act of 1995 is enacted. Thus, state and federal legislators appear willing to take these issues into their own hands.

Selected Statutes Applicable to Computer Networks and Privacy

> Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men.[234]

Federal Statutes and Laws

> The world's information base … [is] estimated to be doubling every three to four years[235]

"As the information privacy of individuals becomes increasingly threatened by the heightened use of computers by the government, the Congress enacted statutes to provide individuals control of some amount of privacy."[236] The federal statutes involved are the Freedom of Information Act, Communications Decency Act, Electronic Communications Decency Act, Cox-Wyden Bill, Code of Fair Information Practice, and the Privacy Act of 1974. The major federal laws on privacy which impact an Acceptable Use Policy are:

The Privacy Act of 1974.[237] The Act was implemented "to provide certain safeguards for an individual against an invasion of privacy." The Act is very

---

[234] Ayn Rand. (1994). The fountainhead. New York: Plume.

[235] David F. Linowes. (1989). Privacy in America: Is your private life in the public eyes? Chicago: University of Illinois Press, page 169.

[236] Right to privacy in the age of telecommunication [On-line]. (1996).

[237] 5 U.S.C.S. §552a, 66 Am. Jur. 2d, Records, §46.5; Pub. L. No. 93-579.

important, but poorly understood, law which "seeks to protect individuals against the misuse of information about them contained in government files."[238] It was born as a result of the Watergate crisis. In 1974, the 93rd Congress considered a number of pieces of legislation dealing with various aspects of privacy. The bills dealt with the regulation of governmental data banks,[239] a wide range of data bases in a number of federal and state agencies dealing with criminal justice information,[240] the disclosure and sale of mailing lists,[241] and various other measures containing access and disclosure provisions for various other statutes.[242] The Privacy Act is a comprehensive response to the public's concern as to just how much information is available about the average citizen and what can be done with such data.

The federal government had been gathering information on the average citizen for decades without drawing the concerned attention of the citizenry. Two factors (which made Watergate possible) heightened the concern of the public to such a degree that legislation was in order. First, the federal government had been growing larger each year, and thus the amount of information it collected had grown in order to make informed policy decisions possible. Second, the maturation of technology had made the compilation, retrieval, analysis, and dissemination of data significantly easier. Previously, all of this has been required to be done manually.[243]

During the Congressional hearings which recommended the enactment of the Privacy Act, a 1974 study of 54 federal agencies revealed the existence of over 800 computerized data banks containing some 1.25 billion records on individual citizens.

---

[238] Creech, Kenneth C. (1993). Electronic media law and regulation. Boston: Focal Press, page 256.

[239] S. 3633, 93d Cong., 2d Sess. (1974).

[240] S. 2963, 93d Cong., 2d Sess. (1974).

[241] S. 3116, 93d Cong., 2d Sess. (1974).

[242] S. 2452, 93d Cong., 2d Sess. (1974).

[243] See generally, Note, The Privacy Act of 1974: An Overview and Critique, 1976 Wash. U. L.Q. 667.

The Federal Bureau of Investigation's main data bank (the National Crime Information Center - the NCIC) then contained just under 2 million files and almost 200 million sets of finger prints. It was also discovered that some 30 data banks exist which contained information about political and other such activities of many thousands of law-abiding citizens. One expert who testified before the Congress estimated that the typical citizen was the subject of at least 20 records.[244]

The Act addresses the gathering and possible misuse of otherwise personal information, and very clearly expresses its intention in section 2 where it states:

> The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;
>
> The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information;
>
> The opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuses of certain information systems;
>
> The right to privacy is a personal and fundamental right protected by the Constitution of the United States, and;
>
> In order to protect the privacy of the individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use and dissemination of information by such agencies.[245]

The Privacy Act's purpose was "to provide certain safeguards against an invasion of personal privacy."[246] To accomplish this the Act has six basic provisions:

- Individuals are given control over what personal records[247] (pertaining to themselves) can be collected and maintained by the Federal government.

---

[244] Note, The Privacy Act of 1974: An Overview and Critique, 1976 Wash. U. L.Q. 667, 670.

[245] Privacy Act, Pub. L. No. 93-579 (1974).

[246] Privacy Act, Pub. L. No. 93-579 (1974).

[247] 5 U.S.C. §552a(a)(4) considers a "record" to be: "any item, collection, or grouping about an individual that is maintained by an agency, including, but not limited to his education, financial transactions, medical history, and criminal or employment history, and that contains his name, or

- Individuals have control over the dissemination of personal records gathered by one agency when other organizations or agencies request that information.
- Individuals can gain access to their records in any agency and can have such information corrected or amended.
- Agencies are required to assure that all information is current and accurate for its intended use.
- Agencies are exempted from other provisions of the Act "only in cases where there is an important public policy need for such exemption."
- Agencies violating an individual's rights under this Act are subject to civil litigation by the individual.

The Electronic Communications Privacy Act of 1986 (ECPA). The ECPA[248] contains two main parts or *Titles*. Title I deals with "Interception of Communications and Related Matters." This Title updates existing laws to encompass computer 'acts' as illegal if there is an equivalent real life law. For example, where the law is such that you can not electronically eavesdrop on private telephone communications, it now states that you can not electronically eavesdrop on private computer communications. Where the law preserved your right to *listen* to public radio transmissions, it preserves your right to *listen* to public computerized transmissions.

Title II deals with "Stored Wire and Electronic Communications and Transactional Records Access." This Title makes certain acts federal crimes. Equally important, it protects certain common-sense rights of system operators (sysops). Under the Act, it is now a federal offense to access a system without authorization.

The Cox-Wyden Bill. The Cox-Wyden Bill (Internet Freedom and Family Empowerment Act) on August 4, 1995 was passed by the US House of Representatives "as a direct response to the Prodigy decision and the original version

---

the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."

[248] Electronic Communications Privacy Act of 1986, Pub. L. 99-508 (1986).

of the Communications Decency Act."[249] The bill specifically prohibits the Federal Communications Commission (FCC) from regulating material on the Internet.[250] It released access providers from liability if they did not exercise direct editorial control over their transmissions. The bill ensured that access providers could unilaterally remove obscene material without incurring liability, provided there was a "good faith" effort to screen services, and provided screening devices for parents.[251]

"By prohibiting FCC intervention, the Cox-Wyden bill virtually eliminated the prospect of federal content-based regulation of the Internet. It focused on screening indecent material from children, instead of regulating or eliminating the material from the Internet altogether."[252] The bill attempted to "remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material . . ."[253] "[T]his bill was favored by on-line users and access providers. The latter were shielded from liability, while the former continued to enjoy a decentralized and uncensored Internet."[254]

> The Cox-Wyden bill failed to directly address the concerns of parents and teachers regarding children's continued Internet access to indecent and obscene materials. The bill's focus on screening devices carried a less powerful punch than its proponents would have liked to admit. The bill's language merely provided that as a general "policy," the government should "remove disincentives" for the development of screening and blocking devices. This language is suggestive, but vague. It did not mandate any behavior or specific actions by access providers to

---

[249] Caden and Lucas at para 56.

[250] 141 Congressional Record. H8478-79 (August 4, 1995).

[251] H.R. 1978, §230(c), 104th Cong., 1st Session (1995) ("No provider ... shall be held liable on account of -- (1) any action voluntarily taken in good faith to restrict access to material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected ...").

[252] Caden and Lucas at para 57.

[253] H.R. 1978, §230(b)(4), 104th Cong., 1st Session (1995)

[254] Caden and Lucas at para 58.

> further this policy. For those who feel that FCC jurisdiction may be appropriate, the Cox-Wyden bill failed to grant proper control over the medium.[255]

The House-approved Cox-Wyden bill preserves the Internet as a more-or-less, unregulated environment which appears to be an outcome desired by civil libertarians and many Internet users.[256] But the Communications Decency Act held center stage and a majority of the Cox-Wyden bill was incorporated into the adopted version of the CDA, "with the notable exception of Cox-Wyden's prohibition on FCC jurisdiction. In lieu of the Cox-Wyden approach to FCC jurisdiction, the CDA grants the FCC a consultative role in helping determine appropriate standards for indecent material available on-line."[257] Nonetheless, the FCC, under the adopted CDA, is prohibited from enforcing those standards.[258]

The Freedom of Information Act (FOIA). The FOIA stipulates that "every American has the right to look at any government records unless the disclosure of a record would warrant an"[259] "invasion of personal privacy."[260] "This act gives the citizens the right to know what the government knows so that the citizens would be able to discover any fraud in the government, including privacy violations."[261] "Ironically, this act simultaneously creates a tension between the public's right to

---

[255] Caden and Lucas at para 58.

[256] See e.g.. John Perry Barlow. (1994, March). The economy of ideas: A framework for rethinking patents and copyrights in the Digital Age. Wired, 2.03. Available as of July 1, 1996: http:// www.hotwired.com/wired/2.03/features/economy.ideas.html; Also see, Caden and Lucas at para 59.

[257] Caden and Lucas at para 59.

[258] Communications Decency Act §502.

[259] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).

[260] Freedman. Warren. (1987). The right of privacy in the computer age. New York: Quorum Books. page 18.

[261] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).

know and an individual's right to privacy."[262] The Act allows files to be available to any person, thus individual privacy may be lost. The Act does attempt to protect the privacy of individuals by making certain categories of data not readily accessible. However, the Act, in regard to "internal personnel rules," or, "files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" the Act is vague.[263] This vagueness "create[s] interpretational problems, especially with the use of computers."[264]

> For example, what constitutes *files* remains ambiguous when using a computer. Should *files* be interpreted to constitute storage discs or data cells containing items unrelated to each other? Answering this question determines how much information a person could obtain and how much privacy of an individual can be lost.[265]

Communications Decency Act of 1995 (CDA). The CDA[266] was approved by the U.S. Senate as an amendment to the Senate's omnibus telecommunications deregulation bill. This amendment poses great Constitutional questions in regard to the future of freedom of speech on the computer networks.

The CDA was sponsored by Sen. James Exon (D-Nebraska) and was intended, according to its sponsor, both to prohibit the [computer] equivalent of obscene telephone calls and to prohibit the distribution to children of materials with sexual content. The legislation imposes content restrictions on computer communications that would chill First Amendment protected speech in forums of

---

[262] Freedman, page 18-19.

[263] Richard F. Hixson. (1987). Privacy in a public society: Human rights in conflict. New York: Oxford University Press, page 194-95, 199.

[264] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).

[265] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).

[266] Communications Decency Act of 1995, 47 U.S.C. 151 (1995).

computer networks. The only postings that would be acceptable would be those appropriate for children to read.

The CDA changes the language of Title 47, US Code, Section 223. This section of Title 47 primarily deals with: 1) a prohibition on "obscene or harassing" phone calls and other, similar, abusive uses of the telephone, and, 2) FCC regulation on telephone services that provide so-called *indecent* content, and prohibits those services from providing legally obscene content.

In other words, the CDA substantially restructures and alters the provisions of this section in an effort to bring computer communications under the same laws that effect telephone communications.

The Communications Decency Act of 1995 will, according to the Electronic Frontier Foundation:

> (a) Expand the scope of the statute from telephones to "telecommunications devices" (such as computers, modems, and the data servers and conferencing systems used by Internet sites and by commercial providers like America Online and CompuServe);
>
> (b) Define as a criminal offense any communication that is legally obscene or indecent if that communication is sent over a telecommunications device "with intent to annoy, abuse, threaten, or harass another person";
>
> (c) Penalize any person or entity who, by use of a telecommunication device, "knowingly ... makes or makes available" any content or material that is legally obscene; and
>
> (d) Penalize any person or entity who "knowingly ... makes or makes available" to a person under the age of 18 any content or material that is "indecent."[267]

---

[267] Electronic Frontier Foundation. (1995, June 10). EFFector, 8 [On-line]. Available as of July 1, 1996: http://www.eff.org/pub/EFF/Newsletters/EFFector/#8.

The CDA may very likely be declared unconstitutional as it is vague and overly broad in its mandate. Case law has already been handed down by the Supreme Court which, in all likelihood will undo the CDA. In Sable Communications v. FCC (1989),[268] a case involving dial-in phone-sex services, the Supreme Court held that, even though a ban on obscenity in dial-a-porn services is constitutional, a ban on indecency is not. The Court also said that "[t]he government may not reduce the adult population to only what is fit for children."[269]

The Code of Fair Information Practice (Public Law 93-579, sec 2(b)) was recommended by an advisory committee of the Secretary of the Department of Health, Education and Welfare in a report called Records, Computers, and the Rights of Citizens in 1973.[270] "The code served as the model in constructing the Privacy Act."[271] The five major principles of the code mandate that the government will:

1) create no secret personal data record-keeping systems,
2) provide access for individuals to find out the use and existence of any information about him/her in a record,
3) establish a procedure for individuals to prevent the use of information collected for one purpose to be used for another purpose without his/her consent,

---

[268] Sable Communications vs. FCC, 492 US 115 (1989).
[269] Sable Communications at 121.
[270] Michael Rogers Rubin. (1988). Private rights, public wrongs: The computer and personal privacy. Norwood, MA: Alex Publishing Corporation, page 80.
[271] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).

4) allow an individual to correct a record about himself/herself, and,

5) assure the reliability and accuracy of the use, maintenance, and dissemination of the data.[272]

These principles mandate a number of requirements from the Privacy Act. An individual should be able to:

- determine what records related to him/her are used, collected, maintained, and disseminated,
- prevent the use of information collected for one purpose from being used for another purpose without his/her consent,
- access information pertaining to him/her, have copies of such records, and be able to make corrections.

These stipulations are in place in order to provide for a balance between the individual's rights and the governments interest in collecting data. "In essence, this act empower[s] individuals to know of the existence and use of the information pertaining to them collected and held by the government."[273]

Selected Cases

In Pemberton v. Bethlehem Steel[274] it was held that surveillance is not actionable (as an invasion of privacy) so long as the surveillance is conducted in a reasonable and unobtrusive manner. Thus, the use of software to monitor the size of

---

[272] U.S. Congress, Office of Technology Assessment. (1986). Federal government information technology: Electronic record systems and individual privacy. (Office of Technology Publication No. OTA-CIT-296). Washington, DC: U.S. Government Printing Office, page 16.

[273] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).

[274] Pemberton v. Bethlehem Steel, 502 A.2d 488 (1986), 306 Md. 289, cert den 479 U.S. 984 (1986), 93 L.Ed.2d 575.

user's account space consumption would appear to be legal (even if there is an assumption that the user's account space is totally private).

Stikes v. Chevron USA[275] is a case where a former employee of Chevron brought action based upon his belief that Chevron (and the federal Labor Management Relations Act) breached his Constitutional right to privacy. As part of the Chevron's collective bargaining agreement's safety program, employees were required to submit to random searches of their person and property. Stikes refused to submit to a search of his private vehicle which was parked on company grounds. As a result of his refusal, he was discharged. The case was decided in favor of Chevron, and the Supreme Court upheld that decision from a lower court.

Citing Stikes, a university AUP stating that users, given proper notice, must submit to searches of their accounts would appear to be lawful and not a breach of their right to privacy provided the university has a compelling interest in setting such a policy.

In Barber v. Time the court held that a person does not always have a reasonable expectation of privacy, and that they can not have *complete isolation* under the right of privacy. Individual rights should be construed in the light of the duties and responsibilities incumbent upon citizens of a free country. Thus, a person on a computer system who expects to be totally isolated from intrusion, warranted or unwarranted, is mistaken. Barber also indicates that some intrusions, even if they are unwarranted, are not actionable.[276]

In Elmore v. Atlantic Zayre[277] a store employee (based upon complaints from customers) observed an individual allegedly performing acts of sodomy. The

---

[275] Stikes v. Chevron USA, 914 F.2d 1265 (1990), cert den (US) 59 USLW 3769. 137 BNA LRRM 2248, 118 CCH LC §10703.

[276] Barber v. Time, Inc., 159 S.W.2d 291 (1942), 348 Mo. 1199.

[277] Elmore v. Atlantic Zayre, 341 S.E.2d 905 (1986), 178 Ga.App. 25.

perpetrator was in a closed stall in a public restroom. The court ruled that there was no invasion of privacy nor did the action violate the individual's privacy interests as Zayre's desire to provide crime free restrooms to its customers was a more compelling than the individual's right to privacy.

Elmore is applicable to a university's AUP as it sets a principle. Certainly the facts of the case do not involve any electronic issues. However the principle of law in this case establishes an analogy between the Zayre's restrooms and a university computer system user's account. Based upon this case, an invasion of privacy is not actionable given the organizations desire to maintain a crime-free environment. Elmore also supports the action of store employees to invade otherwise private spaces (a closed stall in a public restroom) where there is a suspicion of illegal activity.

It would also seem that Elmore will allow university computer staff members to enter a user's computer account if there are reports of, among other things, conspicuous disk space consumption, or other suspicious activity.

The means used in an intrusion of privacy are prime factors, according to Hogin v. Cottingham.[278] There is a great deal of weight given to the degree of intrusiveness that was perceived by the victim. The manner in which an 'intrusion' occurs is important. Thus it would seem to follow that, if a computer monitoring program were transparent, then a plaintiff would seem to loose a cause for action based upon the 'intrusiveness' of the alleged invasion.[279]

Privacy and the Elements and Requisites of Liability

> A legal duty so called is nothing but a prediction that if a man does or omits certain things he will be made to suffer in this or that way by judgment of the court—and so of a legal right.[280]

---

[278] Hogin v. Cottingham, 533 So.2d 525 (1988).
[279] Magenis v. Fisher Broadcasting, 798 P.2d 1106 (1990), 103 Or.App. 555.
[280] Oliver Wendell Holmes, Jr., The Path of the Law, 10 Harv. L.Rev. 457, 458 (1897).

There are a number of elements which must be present in order for an invasion of privacy to be actionable. The information accessed must otherwise be private, secluded, or secret,[281] there must be lack of consent by the owner of the facts,[282] and/or the intrusion must involve public disclosure[283] of facts which are otherwise private. *Some* authorities have also held that a physical intrusion or something analogous to a trespass *must* occur.[284]

> Thus, the term 'wrongful', in regard to a wrongful intrusion, does not require that the intrusion itself be wrongful in the sense that there is no right to make the intrusion, but may relate to the manner of making the intrusion.[285]

Thus, another "primary factor in determining whether there has been an *intrusion* in connection with those aspects of a violation of the right of privacy relating to an intrusion upon seclusion is the means used."[286]

Merely entering onto private property is not, by itself, sufficient to institute an action based upon invasion of privacy. An invasion must be highly intrusive and offensive.[287]

There are, however, a number of elements which do not impact the actionability of an 'invasion of privacy.' Whether an 'invasion' was negligent or

---

[281] Dortch v. Atlanta Journal, 405 S.E.2d 43 (1991), 261 Ga. 350.

[282] Leggett v. First Interstate Bank of Oregon, 739 P.2d 1083 (1987), 86 Or.App. 523.

[283] Dortch v. Atlanta Journal, 405 S.E.2d 43 (1991), 261 Ga. 350; Steele v. Offshore Shipbuilding, 867 F.2d 1311 (1989), reh den 874 F.2d 821 (1989) and McCullough v. Offshore Shipbuilding, 874 F.2d 821 (1989).

[284] Garner v. Triangle Publications, 97 F.Supp. 546 (1951), Hogin v. Cottingham, 533 So.2d 525 (1988), McDaniel v. Coca-Cola Bottling, 2 S.E.2d 810 (1939), 60 Ga.App. 92.

[285] 77 C.J.S. Right to Privacy and Publicity 511; Struner v. Dispatch Printing Co., 442 N.E.2d 129 (1982), 2 Ohio App.3d 377, 2 O.B.R. 435, 77 C.J.S.; Right to Privacy and Publicity 511.

[286] 77 C.J.S. Right to Privacy and Publicity 511.

[287] Magenis v. Fisher Broadcasting, 798 P.2d 1106 (1990), 103 Or.App. 555.

purposefully planned is not relevant.[288] Malice is not an essential element.[289] It does not matter if profit is made from the intrusion.[290]

The actionability of an 'invasion of privacy' is *negated* when publicity is given to facts which are already a matter of public record, or to matters otherwise generally discernible through public observation.[291]

Privacy in Our Electronic Society

> In the new electronic age, we are relying more and more on information technology to streamline government, educate our children, make health care more accessible and affordable, and make our businesses more productive and competitive. This rush to embrace a new age of technology must not, however, obscure our ongoing responsibility to protect important information and maintain the personal privacy of citizens.
>
> - Senator John Glenn (D-OH) Chairman, Senate Committee on Governmental Affairs

Privacy is, conceivably, a foundation issue when crafting an acceptable use policy. The determination of what privacy *is* and *what it is not* will lay a foundation for all subsequent AUP formation discussions. There are a number of flavors of privacy, and a University community should come to a consensus on which flavor it desires.

University computer system administrators and users alike will need to understand that which is before them. Cyberspace presents a new mode of thinking about privacy. Both cyberspace and privacy will need to be understood in order to accommodate *how we describe and use information*. This understanding will be

---

[288] Lynn v. Allied Corp., 536 N.E.2d 25 (1987), 41 Ohio App.3d 392; Prince v. St. Francis-St. George Hosp., 484 N.E.2d 265 (1985), 20 Ohio App.3d 4, 20 O.B.R. 4.

[289] Cason v. Baskin, 20 So.2d 243 (1945), 155 Fla. 198.

[290] Garner v. Triangle Publications, 97 F.Supp. 546 (1951), Hogin v. Cottingham, 533 So.2d 525 (1988), McDaniel v. Coca-Cola Bottling, 2 S.E.2d 810 (1939), 60 Ga.App. 92.

[291] Ledsinger v. Burgmeister, 318 N.W.2d 558 (1982).

"based upon electronic models of how information is organized, stored and processed."[292]

The Electronic Communications Privacy Act of 1986 (ECPA) has been a first step in attempting to deal with one aspect of the many heads of the cyberspatial 'Hydra.'[293] The ECPA deals with a computer information system only as traditional mail and telephony. The ECPA began a legal discussion concerning the nature and ramifications of various viewpoints in regard to cyberspace. The ECPA is the first step toward reducing the lack of comprehension about the foundation issues of how we work with information.

We should begin to realize that cyberspace is more than a one dimensional entity. Cyberspace is analogous to many familiar real-life metaphors, not just to one. Cyberspace is analogous to a:

- newspaper
- republisher/disseminator
- common carrier (i.e., telephone)
- traditional bulletin board
- broadcaster
- desk at the office
- desk at home in the den
- free and open frontier (a.k.a. *The Old West*)
- safe deposit box in a bank
- hotel/motel room which one has rented
- fraternity/sorority house

---

[292] Ethan Katsh, Law in a Digital World, 38 Villanova L. Rev. 403 (1993).

[293] A "Hydra" is a mythical multi headed reptile. The analogy is made that Cyberspace is a multi dimensional entity and can be just as dangerous as a Hydra if one does not address and deal with all the heads (facets).

If an on-line computer system *is* like all of these things, how do we legally and ethically deal with this multi-faceted, multi-dimensional environment, and, how do we deal with a situation in which two antithetical metaphors seem apropos?

A legal and ethical blurring occurs due to the lack of consensus among the various stakeholders as to what the 'rules' and metaphors are in cyberspace.

> In the long run, adoption of information technologies will blur the boundaries between citizen and agency and between agency and court. Blurring of these boundaries may necessitate rethinking the definitions of some of the basic events that define the administrative process, public participation and judicial review.[294]

When crafting an AUP, a foundation issue will be the determination of the scope and limits of privacy on a given computer system. A clarification of privacy as a global principle for computers, as a principle for individual systems, as a non-existent principle, or as some combination of these needs to be established before other concerns are addressed. Deciding this will facilitate the process of developing a basis of thought upon which other issues (e.g., computer as a newspaper, office desk, common carrier, broadcaster, etc.) will rely. Establishing the basic notions of *public* and *private* in regard to on-line computer systems is critical in order to build a foundation upon which resolution of other issues will be based.

It is also an issue that many of those rights, especially the right of privacy, have themselves become confused. The metaphors which are conjured through hypotheticals in order to equate a given cyberspatial act to real life situations are, many times, *in conflict and inaccurate*. An act in cyberspace can be, for example, viewed as analogous to a phone conversation. Given the telephony metaphor, one statute applies, but, given the same act and drawing on a traditional mail metaphor, the situation brings another statute into play. Using a telephony metaphor, this act

---

[294] Perritt, Henry A. Jr., The Electronic Agency and the Traditional Paradigms of Administrative Law, 44 Admin. L. Rev. 79, 105 (1992).

may be completely legal while applying the metaphor of traditional mail might cause the act to be illegal.

Also law enforcement agencies are not solidly founded in regard to cyberspatial legal issues. The legal system's insufficient comprehension of cyberspace has routinely caused search warrants to be issued which are overly broad.[295] Complete computer systems have been seized as evidence when only seizure of a copy of the offending material was in order.[296]

The Clinton administration's program regarding cyberspace, as announced by Vice President Albert Gore, incorporated many of the concepts of open competition, universal access, and deregulated common carriage. But Gore said nothing concerning the future of privacy and personal rights, except to cite, among the bounties of the National Information Infrastructure, its ability to "help law enforcement agencies thwart criminals and terrorists who might use advanced telecommunications to commit crimes."[297]

Lacking legal clarity on a number of issues, a University needs to establish policy—its AUP—in order to clarify the 'ground rules' for the entire community of users. Furthermore, as a chief source of litigation is failure to properly prepare for legal eventualities, having an AUP in place will greatly aid in reducing potential exposure to litigation.

---

[295] Dibbell. (1990, July 24). On line and out of bounds, Village Voice, p 27; Jahnke. (1990, November 14). The cops come to Cyberspace. Boston Magazine, page 140; Barlow, John Perry. (1990). Crime and puzzlement [On-line]. Available as of July 1, 1996: http://www.eff.org/pub /Publications /John_Perry_Barlow /crime_and_puzzlement.1. The scope of "Operation Sun Devil" is unclear. Although many wholesale seizures of computer equipment have occurred over the past several years, executed by teams of federal and state agents, some law enforcement officers specifically have disavowed that their particular police action was a part of "Sun Devil." For example, "[f]ederal officials said that the raid on Steve Jackson Games was not part of Operation Sun Devil." Lewis. (1990, September 9). Can invaders be stopped but civil liberties upheld?, New York Times.

[296] Fed. R.Evid. Rule 101(3).

[297] Albert Gore. (1994, January 11). Clinton administration's NII policy in regards to the National Information Infrastructure. Press Conference. Los Angeles, CA.

Regulation of electronic communication has historically been influenced more by market and political forces than by constitutional principles or legal concerns. Current legislative interpretations and trends are not based upon precedents in jurisprudence or upon striking a balance among the legal principles involved. The decisions are generated from the need to provide a practical resolution to an immediate problem.[298]

There *should*, in the short term at least, be a balance between the need to have an immediate and practical solution, and, the desire to have a just and fair solution. After all, application of theoretical law has always been predicated upon its implementation in actual case law. Thus, we should blend the theoretical and the practical.

The National Information Infrastructure's (NII) Working Group Task Force on Privacy supports this blending, as indicated by Carol Mattney's statement on their behalf:

> . . . the Information Infrastructure Task Force's Working Group on Privacy [intends] to update the Code of Fair Information Practices that was developed in the early 1970s. While many of the Code's principles are still valid, the Code itself was developed in an era when paper records were the norm.
>
> The advent of the National Information Infrastructure has caused two things to change dramatically. No longer is information usage bound by the limitations of paper - the seamless web of networks linking us to each other is creating an interactive environment in which all of the participants must share certain responsibilities. Moreover, non-governmental usage rivals the government's [usage], and is largely unregulated.[299]

---

[298] It would be impossible to exaggerate the frequency with which computer information banks containing private information of third parties are seized, ostensibly in search of criminal evidence. Most bizarre is the story of the nonprofit California cryogenics organization, whose computer equipment and cryogenics-related bulletin board were seized and shut down, in the course of a coroner's office investigation into the whereabouts of a missing human head. See Brock Meeks. (1991, April 12). The case of the missing head and the missing BBS. Available as of July 1, 1996: http://www.well.org/finish

[299] National Information Infrastructure Task Force. (1995). Statement on Privacy. Available as of July 1, 1996: gopher://gopher.eff.org/11 /CAF/policies.

Applying long-standing guarantees in the burgeoning electronic forum, Tribe recommends "that policy makers look not at what technology makes possible, but at the core values the Constitution enshrines."[300] The principles of the Constitution, he maintains, are its protection of people rather than places, and its regulation of the actions of the government, not of private individuals. Tribe notes there must be an "invariability of constitutional principles despite accidents of technology."[301] Tribe's statement provides a basis for the belief that government and university administrators should set acceptable use policy instead of allowing it to be established solely by network denizens, as is often currently the case.

> If the primary nature of the role of government and the University's administration is protection, coupled with facilitation, then existing laws, statutes and University policies could well be developed/applied for the protection of privacy when accidents of technology threaten it.[302]

Two points of view appear to exist concerning the broad notion of privacy. On one hand, the Electronic Frontier Foundation (EFF) and the Computer Professionals for Social Responsibility (CPSR) favor almost exclusive privacy from governmental intrusion. On the other hand, the System Administrators want to be able to insure the security and integrity of their on-line systems. The administrators of on-line networks (System Administrators, postmasters, System Operators, etc.) want and deserve the legal ability to protect their systems from vandalism and illegal intrusion, and to prevent them from acting as conduits for pirated software, or serving as homes

---

[300] Laurence Tribe. (1991, March). The Constitution in cyberspace: Law and liberty beyond the electronic frontier. Keynote address at the First Conference on Computers, Freedom and Privacy, Boston, MA. Available as of July 1, 1996: http://www.swissnet.ai.mit.edu/6095/articles/tribe-constitution.txt.

[301] Laurence Tribe. (1991, March). The Constitution in cyberspace: Law and liberty beyond the electronic frontier. Keynote address at the First Conference on Computers, Freedom and Privacy, Boston, MA. Available as of July 1, 1996: http://www.swissnet.ai.mit.edu/6095/articles/tribe-constitution.txt.

[302] Vernon Pero (e-mail communication, June 5, 1994).

for illegal activity. There is legitimate concern that, given free rein, those who craft policy will follow a path that may not consider the rights of the individual users.

Virtual Reality should not be interpreted as a duplication of real life society; but as an extension of it. Separating them in such a way that electronic communications would be completely secure and free from intrusion, while other aspects of one's life are not, seems unreasonable. For example, telephone calls are not currently totally secure, as with proper authorization, the government can wiretap them. One's "person, papers, houses, and effects"[303] are secure only from unreasonable searches, not totally secure from any searches whatsoever.

The University administration has been established to protect everyone's rights and to insure that everyone's rights and responsibilities are properly addressed and protected. The stakeholders in the creation of policy should be constantly reasserting, in their minds, that crafting policy is a positive activity and should benefit and protect all.

Both sides have legitimate and compelling reasons for their points of view. Senator Patrick Leahy notes that "(t)he part that frightens the hell out of me is the government deciding where technology goes."[304] Senator Leahy is reflective of the thinking of those who believe that, left to its own devices, government (or those who govern, i.e., the administration of an organization) will function in its own best interest, and not in the interest of the community which it serves.

In regard to self interest and the direction an organization will take, Herbert Schiller states that "[b]ehind all the hype shaping the electronic highway are

---

[303] U.S. Const. amend. IV.

[304] Senator Patrick Leahy (D-Vermont) quoted in Kevin Power. (1994, April 10). Proposed wiretap law sets off debate over justice role. Government Computer News, page 5.

corporate interests. These huge companies are doing the most natural thing in the world . . . [they are] following their own corporate interest."[305]

Alternatively, FBI Director Louis Freeh asserted that: "in order to keep up with the criminals and to protect our national security, the solution is clear: we need legislation to ensure that telephone companies and other carriers provide law enforcement with access to this new technology."[306]

On May 19, 1994, Director Freeh spoke in Washington, DC, to the American Law Institute. He contended that: "Within the last month, the FBI conducted an informal survey of federal and local law enforcement regarding recent technological problems which revealed over 180 instances where law enforcement was precluded from implementing or fully implementing court [wiretap] orders."

However, EPIC[307] Legal Counsel David L. Sobel disputes the statements of FBI Director Freeh. Sobel stated that the FBI and other such agencies have not yet demonstrated a need for sweeping new legislation such as their digital telephony proposal[308] or the Clipper Chip.[309] Sobel also stated that "[t]he Bureau has never

---

[305] Herbert Schiller. (1994, March). Information superhighway: Paving over the public. Z Magazine, page 21.

[306] Louis Freeh. (1993, December 8). Making new telecom technology wiretappable. Presented at the National Press Club, Washington, D.C.

[307] EPIC (Electronic Privacy Information Center) is a public interest research center in Washington, DC. It was established in 1994 to focus public attention on emerging privacy issues relating to the National Information Infrastructure, such as the Clipper Chip, the Digital Telephony proposal, medical record privacy, and the sale of consumer data.

[308] The FBI digital telephony proposal. (1994, October 6). The Wiretap Watch, 1.05. The 'FBI's Wiretap Bill', mandates that all communications carriers must provide wiretap-ready equipment so that the FBI can more easily implement their court-ordered wiretaps. The costs of re-engineering all communications equipment will be borne by the government, industry and consumers. It does not cover information service providers.

[309] The *Clipper Chip* has been designed and introduced by the Federal government to standardize encryption technology so that law enforcement agencies can listen in on "private" conversations in electronic media. The device will initially be installed in government phones, and AT&T will also sell it for individual and business use. It is clear that the government would very much like the Clipper to become the standard for all future domestic electronic "private" communication. Many respected professionals in telecommunications and related industries fear that the government may soon make moves to outlaw or otherwise kill other encryption technology that could compete with the Clipper Chip.

presented a convincing case that its wiretapping capabilities are threatened. Yet it seeks to redesign the information infrastructure at an astronomical cost to the taxpayers."[310] EPIC also notes that the nation's telephone companies have consistently stated, in all cases, that the needs of law enforcement have been met.

Education in the USA is also aggressively moving forward on a national electronic network which will maintain student records. This network will allow exchanges of information among a vast number of agencies and schools. There will be continuous tracking of individuals through the social service, education and criminal justice systems, into higher education, the military and the workplace. Overlooked in this organizational structure is any assurance that the data will be collected and disseminated only with the knowledge and informed consent of parents. This action seems to violate the federal Family Educational Rights and Privacy Act of 1974 (20 USC 1232g) and related federal regulations.

Absent also is a regime level mindset that lobbies for the rights given to all citizens by the First, Fourth, Fifth, and Fourteenth Amendments of the US Constitution. Purporting to survey the primary goals of 'education', they seem to be establishing as much 'network' as possible and gathering as much information as possible. There appears to be minimal, if any, concern for the nature of the data collected and its relationship to personal privacy.

Efforts are moving forward on a national level. Proposals being implemented include:

- Compiling electronic "portfolios" for all students,
- Requiring enrolling kindergarten students to produce Social Security Numbers, which will track them through high school.
- Providing high school students' transcripts and teachers' ratings (of students) to employers

---

[310] David Sobel (personal e-mail, January 14, 1994).

The National Education '*Goals 2000*' Panel recommends that it is "essential" for school districts and states to collect information on students. This information will include: name, type, and number of years in a institution, duration and extent of first prenatal care, birth weight, preschool program, poverty status, physical, emotional and other development at ages 5 and 6, date of last routine health and dental care, extracurricular activities, type and hours per week of community service, name of post-secondary institution attended, post-secondary degree or credential awarded, employment status, type of employment, and employer name.[311]

This report also calls for the collection of additional "data elements useful for research and school management"[312] such as: names of persons living in student household, relationship of those persons to student, highest level of education for primary care-givers, total family income, public assistance status and years of benefits, number of moves in the last five years, nature and ownership of dwelling.[313]

For example, recent legislation in Washington state (SB 6428, HB 1209, HB 2319) provides direct connectivity between public schools, a social service superagency, and other community agencies which provide family services.

Together We Can, published by the U.S. Department of Health and Human Services and the Department of Education describes this type of program. It also suggests a need to "overcom[e] the confidentiality barrier."[314]

Along the same lines, on July 12, 1994, the *CBS Evening News* reported that the National Commission on Immigration Reform (a bipartisan group formed under the 1990 Immigration Reform Act) was about to recommend that a national identity

---

[311] Goals 2000: Educate America Act, Pub. L. No. 103-227 (1994).
[312] Goals 2000.
[313] Goals 2000.
[314] U.S. Department of Health and Human Services and U.S. Department of Education, (1993). Together we can: A guide for crafting a profamily system of education and human services. Washington, DC: U.S. Government Printing Office.

card be adopted. This card would be used to verify employment eligibility and to expedite other actions with government agencies. Each photo-id card would contain a name, fingerprints, and a verified Social Security Number.

CBS reported that this action was supported by long-time national-ID-card advocate Senator Alan Simpson (D-Wyoming). The national ID-card idea is not, by any means, the idea of a solitary few. California Gov. Pete Wilson has offered to make California a test-bed for the proposal.

The Secret Service has testified before Congress that a such an national ID card system development would cost approximately $2 - $4 billion. The Secret Service also noted that within a few months of implementation of such a system, forged cards would be readily available.

The Commission said that its mandate was to inquire into a "simple, fraud resistant way of verifying authorization to work, building on information the government already maintains..."[315]

In order to function, in the future, in our democracy, we should define what privacy is and what privacy is not in cyberspace. There should be a balance between a user's expected right to privacy and the administration's right to insure the continued operation of its systems. This balancing should be crafted into an AUP in order for it to be effective.

Violations to the Right of Privacy

> The fear of invasion of privacy lies in the real possibilities and/or occurrences of misuse of advancing technology. The abuse from either a big institution, such as the government, or a private individual can easily deprive unsuspecting victims of privacy. Although the types of intrusion may differ depending on the size, number, and the intention of invaders, the results all point to the common denominator--privacy loss.[316]

---

[315] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).
[316] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).

Current technology allows access to databases to gain information about an individual for the sake of knowledge, or to manipulate private information for an organization's profit. On the other hand, private individuals may simply invade another's privacy for amusement or for the pleasure of manipulating the technology. With the integration of the computer into the information superhighway, more threats to privacy invasions arise.

The statistics (see figure 3) show that the public understands the existence of the threat of losing privacy to the government or to an equally equipped employer. The examination of the types of invasions of privacy possible by such organizations will illuminate the possibilities of electronic monitoring through wiretapping and data matching. The increased incorporation of the Internet into today's communication systems also raise the same kind of threat which electronic surveillance via the Clipper Chip controversy reflects.

Wiretap Surveillance

> Almost one out of every ten Americans believes his or her telephone has been tapped at one time or another[317]
>
> Congress intended that wire surveillance be difficult.[318]

"In today's society where the use of telephone has become ubiquitous, wiretapping can provide a valuable aid for catching criminals in the act or for simply giving the tapper important information for personal gain."[319] Wiretapping is capable

---

[317] William Petrocelli. (1981). Low profile: How to avoid the privacy invaders. New York: McGraw-Hill Book Company, page 179.

[318] Branscomb, page 36.

[319] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).

of depriving individuals of their privacy, as a person may not have knowledge that a third party is listening to and/or recording the conversation. Tuerkheimer[320] believes that people have "an expectation of privacy" when making telephone calls. Therefore, the possibility of an unwanted party monitoring private conversations is quite upsetting. Such is generally not the case on the Internet. People do not appreciate what privacy is like in cyberspace, let alone have an expectation of privacy.

The current wiretap statute has *de facto* loopholes that leave sizable room for invasion of the privacy of an unsuspecting phone caller. Although, according to the notice in the telephone company's *White Pages*, "calls between customers are not monitored for [training and quality control purposes] or for any purpose ... except when required by law enforcement and national defense agencies," however, if the telephone company spots suspicious calls, the telephone company may inform the law enforcement agencies of suspicions of criminal activity so that the law enforcement agents can obtain a warrant to tap the phone line. Although the statute requires the federal agencies to obtain a search warrant in order to tap a line, telephone company is exempted from obtaining any search-warrants for routine monitor.[321] As a result, in one incident, the telephone company monitored about 1.8 million telephone calls for five years, justifying its action as necessary to catch Phone Phreaks.[322] Unfortunately, more than 98% of the calls monitored were *innocent*.[323]

---

[320] Frank M. Tuerkheimer. (1993, August). The underpinnings of privacy protection. Communications of the ACM, 36(8), page 36.

[321] William Petrocelli. (1981). Low profile: How to avoid the privacy invaders. New York: McGraw-Hill Book Company, page 183.

[322] Petrocelli, page 180.

[323] Petrocelli, page 180.

Petrocelli also reported that telephone company employees routinely listen to telephone conversations under the guise of maintenance and training.[324]

Even though wiretap law stipulates that phone companies should assist law enforcement agencies in executing warrants for wiretap, the law does not provide for unofficial surveillance by the telephone company. [325] However, it is difficult to stop such surveillance because the existing law exempts the phone-company employee in routine monitoring of the calls.[326] Hence, unofficial surveillance can occur in the disguise of routine monitoring.[327]

The loopholes in the existing wiretap laws allow room for loss of privacy for individuals caught unsuspectingly. Granted that "wiretapping has been a critical tool in combating organized crime, drug trafficking, and acts of extortion, terrorism, kidnapping, and murder,"[328] the potential for wiretapping to not only intrude but monitor individuals weighs heavily in today's society. One can argue that, when people use the phone, they should assume that "the contents of their private phone calls can be revealed by a telephone workman who wanders across their line."[329] "In fact, perhaps people should assume that no privacy will be given when making any phone calls."[330]

> The extension of the telecommunication technology from telephones to the Internet not only extends new methods of communicating but also the problems of

---

[324] Petrocelli, page 183.

[325] Marc Rotenberg. (1993, August). Communications privacy: Implications for network design. Communications of the ACM, 36(8), page 67.

[326] Petrocelli, page 184.

[327] Right to privacy in the age of telecommunication [On-line].

[328] Dorothy E. Denning. (1993, March). Wiretapping and cryptography. IEEE Spectrum, 30(3), page 16.

[329] Petrocelli, page 184.

[330] Right to privacy in the age of telecommunication [On-line].

> unwanted surveillance. The same amount of privacy should exist in using e-mail by the same line of logic as using the telephone. However, because of even less law existing to protect privacy rights in using e-mail, privacy invasion problems are rife in the e-mail system.[331]

"In fine historical fashion, the court stated that the legislation should resolve these types of problems by enacting clearer statutes covering e-mail systems."[332]

> In using either a phone or Internet, the problem of violation of privacy remains unresolved because of unclear legislation. Although the system providers claim that maintaining the operation of the systems necessitates routine monitoring, such routine monitoring can easily transform into surveillance which invades the privacy of the users of the systems. As people depend more and more on these technologies for communication, more surveillance will probably take place to secure the systems' operations, and there will be more violations of privacy. The legislature must enact clearer legislation on what should constitute a routine monitoring.[333]

Data Surveillance

> As information-recording processes have become cheaper and more efficient … an appetite for data has intensified, this has been accompanied by a predilection toward centralization and collection of file material. As if responding to something akin to Parkinson's Law, technological improvements in information-handling capability have been followed by a tendency to engage in more extensive manipulation and analysis of recorded data.[334]

Many artifacts of technology (e.g., gunpowder, the automobile, the aeroplane) have been the penultimate examples of a double edged sword's ability to cut in two directions. The computer is no exception. "The power that attracts people to computers has become a nemesis of right to privacy."[335] The ability of the computer to store vast amounts of information for a long time entices the government and large organizations to do just that. However, storing and analyzing that information raises

---

[331] Right to privacy in the age of telecommunication [On-line].

[332] George B. Trubow. (1992, March). When is monitoring e-mail really snooping? IEEE Software, 9(2), page 97.

[333] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).

[334] Arthur R. Miller. (1971). The assault on privacy: Computers, data banks, and dossiers. Ann Arbor, MI: The University of Michigan Press, page 21.

[335] Right to privacy in the age of telecommunication [On-line].

problems concerning privacy as does the mere potential for such analysis and subsequent use.

Due to the fact that the dissemination and interchange of information via computer networks is virtually instantaneous, the computer can become another tool in violating the right of privacy.

The Clipper Chip Controversy

> The government intelligence agencies feared that the widespread use of the almost unbreakable encryption would breed criminal activities. The problem rises not from the growth of criminal activities but from the inability of the government intelligence agencies to break the encryption to detect and catch the culprits.[336]

"One of the privacy concerns involved in the use of the Internet lies in the application of encryption codes to gain as much privacy in using e-mail as using regular mail."[337] To guard against computer hackers who may intercept and read private e-mail, people increasingly use encryption. To make the inaccessible accessible, the agencies proposed the Clipper Chip as the encryption method for people to use. Because the Clipper Chip allows the government to hold the key to decrypt, the controversy ensued between the proponents and the opponents of the implementation of the Clipper Chip. The disagreements surrounding the implementation of the Clipper Chip technology as the last topic in the types of the violations of privacy demonstrates the urgent need for progressive, clearer legislation in consideration of advancing telecommunication technology.

---

[336] Right to privacy in the age of telecommunication [On-line].
[337] Right to privacy in the age of telecommunication [On-line].

The National Security Agency and the National Institute for Standards and Technology designed the Clipper Chip. The system relies on a *key* to encode and decode information. The *key* consists of bits or series of numbers, and an algorithm.[338] "The *keys* would be placed in *escrow* with the two government agencies. The agencies would only be authorized to hand the *keys* to the law-enforcement agencies when *probable cause* to believe that a crime had been committed was demonstrated."[339] "Hence, government agencies would be able to decode if necessary. The controversy stems from this escrow security system of the Clipper Chip and the possibility of the government to abuse the *back door*."[340]

Clipper Chip proponents argue that the proposal allows "law-abiding citizens with access to the encryption they need and [prevents] criminals from using it to hide criminal activity."[341] A Clipper Chip proponent, Dorothy E. Denning states several points in favor of the Clipper Chip proposal:

> Although present law does not explicitly state that communication service providers must incorporate systems which will insure that the law enforcement agents have the capability to intercept data, the law does state that the communication providers must assist those law-enforcement agents with warrants. The law naturally lacks the provision because at the time of the enactment of the law, legislators did not anticipate technological advances. Hence, in today's society, we must interpret the meaning of the word *assist* more flexibly.[342]

The Clipper Chip proposal would require Internet Service Providers (ISPs) to route the monitored traffic to the law-enforcement agents. "[T]he connection to a

---

[338] Dorothy E. Denning. (1993, July-August). The clipper encryption system. American Scientist, 81(4), page 31.

[339] Levin, Carol. (1993, November 23). Digital privacy: Who has the right to read your data? PC Magazine, 12(20), page 29

[340] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).

[341] Levin, page 29.

[342] Dorothy E. Denning. (1993, March). To tap or not to tap. Communications of the ACM, 36(3), page 27.

remote government monitoring facility would support an outgoing data stream only...[it] does not impose any new or additional danger to the security of the systems and the privacy of the people who rely on them for their communications."[343] Denning postulates that the privacy level will not decrease because the "employees of the service providers who have been strict about requiring court orders"[344] must initiate the surveillance as opposed to law enforcement officials.

The Right to Privacy in the Age of Telecommunications[345] critiques Denning's position when he states that:

> In light of the public concern over intrusiveness of the wiretapping, because of public reaction against the court's inaction, the [Congress] took the action to curb wire surveillance. Although Congress could not have known how far technology would progress, the enactment of the wiretapping law did not intend or imply the facilitation of the wire surveillance for the government agencies. Denning misconstrues this intention by taking the word "assist" out of context. The basic purpose of enacting the wiretapping law is to allow as few wiretaps as possible, not to aid the intelligence agencies in wire surveillance.[346]

In reality, the threat to privacy will not diminish, and may well increase. The Clipper Chip proposal does not attempt to reduce such risk. Warren and Brandeis[347] note in their 1890 law review article that privacy is diminishing.[348] Even with governmental reassurances and safeguards the public must have "more than a huge leap of faith … to entrust government agencies with the keys to the encryption."[349]

---

[343] Dorothy E. Denning. (1993, March). To tap or not to tap. Communications of the ACM, 36(3), page 28.

[344] Dorothy E. Denning. (1993, March). To tap or not to tap. Communications of the ACM, 36(3), page 28.

[345] Right to privacy in the age of telecommunication [On-line].

[346] Right to privacy in the age of telecommunication [On-line].

[347] Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

[348] Warren and Brandeis at 202.

[349] Right to privacy in the age of telecommunication [On-line].

In support of the Clipper Chip, Marc Rotenberg indicates that that the intelligence community (e.g., CIA, military intelligence entities) and law enforcement agencies (FBI, state police, state bureaus of investigation) only want access, not remote monitoring capability, simply does not obviate the fact that the proposal intends to set up a "government monitoring facility."[350]

> By endorsing the monitoring capability, people cannot expect privacy even though the quintessential reason for using the encryption is for privacy. Hence even if by practice those who use the system will not lose privacy, people will not expect privacy to be preserved because people will perceive the omnipresent monitoring capability of the government in using the Clipper Chip. This apprehension violates the privacy of the Clipper Chip users by changing the perception of the degree of privacy maintained or not maintained. The users lose a sense of freedom and personal space. By losing certain personal space, the users will also lose some privacy.[351]

Clearly the government is charged with the duty to protect its citizens from harm and illegal activity. So, too, is a university administration duty-bound to insure, *inter alia*, that the computer system is protected from attack and is managed in a fair and equitable manner. "But the cost of protection must not come at the expense of the rights unconsented by the individuals."[352] To balance the right of privacy against the government's power to protect "shifts the balance of power and control to...[the] government."[353] This shifting of power in favor of the government brings into serious question the principles of the social contract drawn by the founding fathers in the Constitution.

---

[350] Rotenberg, Marc. (1993, August). Communications privacy: Implications for network design. Communications of the ACM, 36(8), page 38.

[351] Right to privacy in the age of telecommunication [On-line].

[352] Right to privacy in the age of telecommunication [On-line].

[353] Michael Godwin. (1993, March). To tap or not to tap. Communications of the ACM 36(3), page 35.

Unfortunately, in electronic communication, the escrow *keys* to the encryption would open "not only the phone line but the filing cabinet"[354] and the resulting loss of privacy coupled with the government's ability to more freely wander about in the personal (and otherwise private affairs) of the public would be seriously out of balance.

This grim picture is the worst scenario; at the moment, the government asserts that it has no intention of mandating the Clipper Chip.[355]

> However, painting the extreme worst case scenario elucidates how much privacy rights can be violated. Although the argument for not accepting the Clipper Chip cannot depend on the potential of the worst case, the picture focuses on the method and the extent of the privacy violations that can occur. Even if the government chooses not to monitor to the extreme, the frightening fact still remains that the use of the Clipper Chip will result in privacy loss.

The Assessment of Surveillance Problems

> Surveillance constitutes only a part of the issues of privacy invasions in the telecommunications. Disregard for privacy rights have pervaded the mentality of the individuals as well as the big organizations. (e.g. computer hacking, eavesdropping, etc.).[356]

Wiretapping, data manipulation, and the Clipper Chip proposal appear to provide a readily available means by which invasion of privacy rights through surveillance may occur. "The continued expansion and the greater use of telecommunication technology creates new opportunities for abusing the advancing technology at the expense of privacy rights."[357]

---

[354] Barlow, John Perry. (1993, November). A plain text on crypto policy. Communications of the ACM, 36(11), page 24.

[355] John Perry Barlow. (1993, November). A plain text on crypto policy. Communications of the ACM, 36(11), page 24.

[356] Right to privacy in the age of telecommunication [On-line].

[357] Right to privacy in the age of telecommunication [On-line].

Growth of the Internet (see figure 2) causes many troubling questions to arise such as concerns regarding the "status and the level of control of the service providers such as Prodigy."[358] Although civil liberty "groups such as Electronic Frontier Foundation and Computer Professionals for Social responsibility currently battle the issues of many individual rights (including privacy rights) in using the Internet,"[359] the right to privacy is legally 'in limbo' until clear and focused legislation defining the right to privacy in the context of telecommunication technology is enacted.

General Discussion of Privacy

> Since 1988, computer network security breaches have grown dramatically, increasing 50% per year on the Internet—today's information highway. The ability of the government to protect Americans' most private information is at stake. For example, the Internal Revenue Service is among those agencies who rely increasingly on computer networks for such things as filing tax returns. Anyone who pays federal taxes has to wonder who might be browsing through his/her personal financial data.
>
> - Senator William V. Roth, Jr. (R-DE), Ranking Republican, Senate Committee on Governmental Affairs

Throughout its history the United States has contained a great dilemma within its legal and philosophical system. The problem is its need to create a system that protects everyone equally. This is a major difficulty when so many disparate groups exist. The dilemma is one of trying to balance an individual's right to privacy against the public's *right to know*. The Constitutional dilemma between a person's right to privacy and the public's right to know invokes the concept of America itself. We appear to be constantly wrestling with this issue—cyberspace appears to be no exception.

---

[358] Deborah Branscum. (1991, March). Ethics, e-mail, and the law. MacWorld, 8(3), page 67.

[359] Herb Brody. (1992, November-December). Of bytes and rights. Technology Review, 95(8), page 24.

Warren and Brandeis, for all practical purposes, created the modern notion of privacy in their 1890 Harvard Law Review article entitled The Right to Privacy.[360] They recognized the need for constant refinement and development of this right and stated that the idea "that the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and intent of such protection."[361]

There should be a balance between a user's expected right to privacy and the administration's right to insure the continued operation of its systems. This balancing should be crafted into an AUP in order for it to be effective.

The Role of Search and Seizure in Regard to Computer Networks

> Today, the degradation of the inner life is symbolized by the fact that the only place sacred from interruption is the private toilet.
>
> - Lewis Mumford, The Culture of Cities, ch. 1, sct. 5 (1938).

Introduction

The Computer—technology's latest tool in communications—has forced us to re-engineer our policy in regard to the balance between individual privacy and society's need for information. The new communications technology has ushered in a new era of global access where even the least powerful in society have a significant voice. However, the technology has generated the possibility that corporations and

---

[360] Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).
[361] Samuel Warren and Louis Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

the government will be the beneficiaries of Orwellian powers. The outcome of this will be determined by the underlying societal values, and not by the technology itself.

Sergent notes that this is an "apparent …clash between data privacy [concerns] and law enforcement's need to gather evidence in criminal investigations."[362]

In recent years, it has become apparent that we have an ever diminishing degree (and amount) of control over what personal information of ours is available - and available to just about anyone.[363] Neither the law enforcement establishment nor society in general seems to have kept fully abreast of the changing technological times. As a result, our privacy has been severely eroded. Unless a better understanding is achieved in regard to the relationship of cyberspace to our real world paradigms, we may soon find that 'privacy' is non-existent. In regard to search and seizures, 'privacy' is the 'line in the sand' which may not be crossed without a search warrant.

Sergent notes that the "Supreme Court's reliance on risk analysis and its avoidance of the normative questions underlying individual privacy expectations make it difficult to predict how it will decide future Fourth Amendment cases involving computerized information."[364] Sergent also advocates for a "framework by which the

---

[362] Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (1995).

[363] Larry Tye. (1993, September 5). Privacy lost in high-tech era. Boston Sunday Globe, page 18-19. This article detailed the extent to which supposedly private information was actually publicly available in this day in age.

[364] Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (1995).

Fourth Amendment can be applied to a range of activities involved in computer investigation without hampering the legitimate needs of law enforcement."[365]

To develop these frameworks, Sergent suggests that the Supreme Court should extend its current analysis:

> ... of the scope and content of the Fourth Amendment to [include] searches and seizures of computer information. Because the level of privacy we enjoy in personal information depends upon value choices made by our society, examining legal norms is an important part of the process of making those choices. As new technology evolves, the Supreme Court's Fourth Amendment methodology is likely to favor security over privacy. The model [put in place should involve] more emphasis to privacy.[366]

Kapor and Godwin[367] warn of computer searches and seizures based upon the American Bar Association's (ABA) Criminal Justice Section suggested search and seizure guidelines. Kapor and Godwin are concerned that the ABA's position amazingly seems to be based upon three publications from the Department of Justice's National Institute of Justice. Kapor and Godwin note that:

> 1. There was no guidance to the magistrate as to when the computer or related equipment should not be seized, either because it is not necessary as evidence or because such a seizure would intolerably *chill* the lawful exercise of First Amendment rights or abridge a property owner's Fourth Amendment rights.
>
> 2. There was inadequate recognition of the business or individual computer owner's interest in continuing with lawful commercial business, which might be hindered or halted by the seizure of an expensive computer.
>
> 3. There was no effort to measure the likelihood that investigators would find computers equipped with such justice-obstructing measures as automatic erasure

---

[365] Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (1995).

[366] Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (1995).

[367] Mitchell Kapor, and Michael Godwin. (1994). Civil liberties implications of computer searches and seizures: Some proposed guidelines for magistrates who issue search warrants [On-line]. Available as of July 1, 1996: http://www.eff.org/pub/Publications/Mike_Godwin /search_and_seizure_guidelines.eff.

> software or *degausser* booby-trapped hardware, the presence of which might justify a no-knock search and seizure, among other responses.[368]

Privacy and Possessory Interests

The Fourth Amendment to the US Constitution forbids unreasonable searches and seizures. The government, if it wishes to intrude into protected (private) areas, should conduct itself within the Constitutional definition of reasonable search. The Supreme Court has strictly limited the definitions of the terms *search* and *seizure* as foundations of the issue of *reasonableness*. Therefore, it is necessary to demonstrate how searches and seizures of computer hardware and data fall within the scope of the Fourth Amendment.

The word *search* and the word *seizure* are not synonymous.[369] Under the law regarding searches and seizures, the term *search* implies that there is a prying into a hidden place for something that might be concealed there.[370] For the purposes of crafting a university AUP, the notion should be established throughout the AUP that 'personal property rights' as we know them in the real world do not necessarily apply to a university computer system.

A user should understand that his/her account on a university computer system is not analogous to his/her domicile or physical person. University computer space is metaphorically, far more like a *public place* than a *private place*; it is likely not metaphorically akin to, for example, a person's university dormitory room.

If this concept is established in the AUP, then it would follow that it is not a *search* (an exploratory investigation) when one observes that which is in an open non-private place.[371] This concept would allow system administrators to have access to a

---

[368] Mitchell Kapor, and Michael Godwin. (1994). Civil liberties implications of computer searches and seizures: Some proposed guidelines for magistrates who issue search warrants [On-line].

[369] State v. Raymond, 142 N.W.2d 444, 449 (1966).

[370] Lindsey v. State, 204 N.E.2d 357, 362 (1965).

[371] State v. Griffin, 202 A.2d 856, 861 (1964), 84 N.J.Super. 508.

user's account in the same manner that any person would be able, in real life, to access a public space. There would be no need for a search warrant.

A Definition of *Seizure*

The U.S. Supreme Court has defined *seizure* as a "meaningful interference with an individual's Possessory interest in that property."[372] For computer networks, this creates an interesting situation as data can be *seized* (actually copied to another disk or tape) and the computer system will, seemingly, suffer "no meaningful interference"[373] as defined in United States v. Jacobsen. Computer files and data are intangible, and it is difficult to envision a 'seizure' occurring when something is copied as opposed to a seizing of the original. However in Katz v. United States[374] and LeClair v. Hart,[375] the courts found that intangible objects and the information which they contain could be held as a *seizure*, even though the original documents were themselves not taken from their owner.

On the other hand, law enforcement officials routinely copy serial numbers from objects, and this has been held not to be a seizure, as it does not meaningfully

---

[372] United States v. Jacobsen, 466 U.S. 109, 113 (1984); see also United States v. Karo, 468 U.S. 705, 712-13 (1984) (The installation of a beeper in a container was not a seizure when it did not meaningfully interfere with the defendant's possessory interest in that container).

[373] United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[374] Katz v. United States, 389 U.S. 347 (1967) (The Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any technical trespass under ... local property law.)

[375] LeClair v. Hart, 800 F.2d 692, 696 (1986) (This case held that a seizure occurred when an Internal Revenue Service agent photocopied documents that were not removed from the owner's possession).

interfere with the owner's Possessory[376] interest.[377] In Bills v. Aseltine,[378] the court held that taking photographs of a search scene was not a seizure. Sergent states that by "literal extension, this approach could leave copying of computer files outside the bounds of Fourth Amendment regulation. The Court might say that the information was not seized because it remains available to its owner."[379]

However, the Supreme Court had previously ruled otherwise in Katz when it found that a wiretap did constitute a *seizure of a conversation*. Sergent reconciles the seeming conflict between Katz and Hicks by arguing:

> ...the Possessory interest in a document or conversation consists of controlling the dissemination and use of the information contained therein, whereas the Possessory interest in an tangible item, such as a stereo, lies almost entirely in its use. Copying the information from a document or conversation interferes with control and thus interferes with the Possessory interest. Photographing a scene or copying a serial number, on the other hand, does not meaningfully interfere with possession. Because the value of a computer file lies in the information therein, it is much more analogous to a written document or oral conversation. Although Hicks could logically extend to all intangible information, copying a computer file should constitute a seizure under the Fourth Amendment.[380]

The question of whether or not copying computer files and data is a seizure will become a more important issue as the use of computers for storing such information increases and as more illegal activity occurs in this circumstance.

This question has not often arisen in courts. As Sergent notes:

> First, police have generally preferred to confiscate the equipment containing the information, rather than simply copying the information itself. Clearly, confiscation of equipment constitutes a seizure.

---

[376] *Possessory Interest* is a person's right to exert control over property in which they have ownership of.

[377] Arizona vs. Hicks, 480 U.S. 321 (1987).

[378] Bills vs. Aseltine, 958 F.2d 697, 707 (1992) (The recording of visual images of a scene by means of photography does not amount to a seizure because it does not meaningfully interfere with any possessory interest.)

[379] Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (1995) at 1185.

[380] Sergent at 1130.

> Second, examination of the physical storage media is usually considered a search, dispensing with the need to discuss whether a seizure occurred as well. Finally, even if copying information does not constitute a seizure, in many instances the police will want to remove the information from the defendant's possession entirely. Such a removal would clearly be a seizure.[381]

It is difficult, at best, to attempt to proffer a legal definition of *seizure* as it pertains to a computer network user's data and/or files.

A Definition of *Search*

> The special protection accorded by the Fourth Amendment to the people in their "persons, houses, papers and effects," is not extended to the open fields. The distinction between the latter and the house is as old as common law.[382]

The legal definition of a *search* is quite vague. The Constitutional meaning of the term *search* is certainly much more difficult to define than is the term *seizure*.[383] Prior to 1967, Olmstead[384] mandated that there must be an intrusion into a constitutionally protected place before a search could occur.[385] This meant that a "search" was area-based.[386] In the age of electronic communications, the Olmstead decision was wholly inadequate. The Olmstead court held that eavesdropping on a person's telephone conversation by use of a telephone tap did not violate the Fourth Amendment's search clause as the wires themselves were not part of the defendant's home. Thus, absent any physical intrusion into the defendant's home (a specific area), there was no search and therefore no search warrant was needed.

---

[381] Sergent at 1186.

[382] Hester v. United States, 265 U.S. 57, 59 (1924) (Oliver Wendell Holmes, Jr., J.).

[383] Wayne R. LaFave, (1987/1994). Search and seizure: A treatise on the Fourth Amendment (2nd ed.). St. Paul, MN: West Publishing. Due to the number of possibilities for police action, the Supreme Court has not proffered a comprehensive definition of the term *search*.

[384] See, Olmstead v. United States, 277 U.S. 438 (1928).

[385] See generally, Katz v. United States, 389 U.S. 347 (1967).

[386] Silverman v. United States, 365 U.S. 505, 510 (1961).

Then in 1967, Katz v. United States[387] reversed Olmstead as to the 'area-based' analysis. Katz' central point was that the search is dependent upon a individual's expectation of privacy in regard to the object or area to be sought in a search. Katz caused the Fourth Amendment to apply directly to individuals rather than specific places. Speaking in support of the majority opinion, Justice Harlan delineated the accepted standards for a *search*: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable."[388]

The first standard which Justice Harlan defined is easily overcome by making an advanced public announcement(s) of the surveillance mechanism/intention. Amsterdam has suggested that the government could diminish a person's subjective expectations of privacy by regularly announcing that comprehensive electronic surveillance was in place.[389] There would then be no expectation of privacy, as everyone would be warned that someone or something would always be monitoring their activity.

Sergent notes that:

> Little attention has been given to the independent significance of the subjective test, so it is not clear exactly how it should be interpreted. Because the subjective expectation of privacy has been so little discussed, and because it is so context specific, it is of little use in applying the Fourth Amendment to future situations.[390]

The second factor in Justice Harlan's test is *objective reasonableness*. Objective reasonableness is a value judgment based determination of how much privacy a person may reasonably expect in today's society.[391]

---

[387] See generally, Katz v. United States, 389 U.S. 347 (1967).

[388] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). This standard has since been adopted by a majority of the Court; See also, California v. Ciraolo, 476 U.S. 207, 211 (1986); Smith v. Maryland, 442 U.S. 735, 740 (1979).

[389] Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 384 (1974).

[390] Sergent at 1186.

[391] See generally, Katz v. United States 389 U.S. 347 (1967).

As Justice Harlan noted in his dissent in United States v. White:

> We should not ... merely recite the expectations and risks without examining the desirability of saddling them upon society. The critical question ... is whether under our system of government ... we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement.[392]

Through the years the Court has been hesitant to make an explicit decision based upon this 'risk analysis' (how much privacy can a person reasonably expect to have). The Court typically asks if the affected individual should have expected that he/she would be undisturbed.[393] In California vs. Ciraolo, Mr. Justice Powell stated that the *reasonableness* of the action should be the concern of law enforcement rather than the affected individual.[394]

As Mr. Justice Thurgood Marshall noted in Smith vs. Maryland,[395] another issue here is that the Court has chosen to view privacy as a "discrete commodity, possessed absolutely or not at all."[396] In Katz, the Court stated that what "a person knowingly exposes to the public ...is not a subject of Fourth Amendment protection."[397]

This rationale of 'knowing exposure' is problematic in that it has been extended such that even disclosure of a bit of information causes one to completely loose Fourth Amendment protection of the information in question. It should not be

---

[392] United States vs. White, 401 US 745 (1971) (Harlan, J., dissenting).

[393] Rakas vs. Illinois, 439 US 128, 143, 148-49 (1978); Katz vs. US at 353. The Court essentially declared that a person who discloses something to another person assumes (unto themselves) the risk of losing protection under the Fourth Amendment.

[394] California v. Ciraolo, 476 U.S. 207, 224 (1986) (Powell, J., dissenting) The Court fails to acknowledge the qualitative difference between police surveillance and other uses made of the [public] airspace.

[395] Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court ruled that a person placing a call has no "reasonable expectation of privacy" that the telephone company will not reveal the fact of the call to third parties, therefore, no warrant was required.

[396] John M. Junker, The Structure of the Fourth Amendment: The Scope of the Protection, 79 J. Crim. L. & Criminology 1105, 1177(1989).

[397] Katz at 355.

that a person's privacy protection rights under the Fourth Amendment are totally lost merely due to law enforcement's ability to procure (otherwise protected) information from a third party (by any means).

Search is a vague and ill-defined legal term. As Sergent states:

> … if something is accessible or visible to the public, regardless of the chances of the public actually accessing or seeing it, it will be considered to have been knowingly exposed, and therefore be outside any reasonable expectation of privacy. In either case, the individual loses her privacy interest because she has disclosed that information to another party.[398]

The Significance of the Discussion

> The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.[399]

In the People v. Manzi, the court held that if recognizable contraband (which was seized by police) is in open view on a street or other place which can be lawfully entered without a trespass occurring or fraudulent invasion of the right of a person, then there was no search but there was a seizure, and nothing in the federal Constitution inhibits the seizure of property, if the possession of constitutes a crime.[400] It is important to establish a metaphorical correlation between Manzi (and other cases cited below) and computer systems. But in cyberspace, all things appear the same. Hence it is extremely difficult to only view an object and ascertain whether that object is, for example, a hacking program or some harmless utility program.

In the People v. Heath the court held that an observation from concealment or a hidden area which is otherwise open to public access is not an unreasonable search. This, however, is not to infer that reading the content of e-mail is allowable into and out of the computer system to include the monitoring of disk space being utilized by

---

[398] Sergent at 1186.
[399] Marron v. United States, 275 U.S. 192, 196 (1927).
[400] People v. Manzi

any given user.[401] This case would seem to offset an argument that a system administrator may not monitor traffic. The concept in Heath is difficult to apply as monitoring in cyberspace is much more intrusive than it would be in a real-world setting. Cyberspatial monitoring seems to necessarily involve trespassing (at least on a conceptual level).

In People v. Thomas, the court held that it is not a search in the Constitutional sense where observations are made of events happening in plain sight (and made from a place the observers have a right to be).[402] This position was reinforced in State v. Childs, in that the court concluded that no search as defined by the Fourth Amendment occurred where the objects of the observation were in plain view and the police officers made those observations from a place they had a right to be.[403] As in Heath, the difficulty here is also the notion of trespass. Both Heath and Thomas are based on the notion that an illegal intrusion is prevented, in this case, by the no-trespass concept. Such is not true in cyberspace. In the real world, privacy (a physical intrusion) is not protected by privacy statutes as much as it is protected by other laws, such as, trespassing, or, breaking and entering.

It is important, on the part of a university, to establish its position that a computer account is *not* a private secluded place. Establishing *private places* would create a situation where users have a reasonable expectation that their *space* will not be invaded. If the situation is such that the computer users have an expectation of privacy in their accounts, then any rummaging about or intermeddling with privacy is searching within the meaning of the Fourth Amendment.[404]

---

[401] People v. Heath, 72 Cal. Rptr 457, 458 (1968), 266 C.A.2nd 754.
[402] People v. Thomas, 169 Cal.Rptr. 570, 572 (1980).
[403] State of Arizona v. Childs, 519 P.2d 854, 856 (1974), 110 Ariz. 389.
[404] State of Maine v. Barclay, 398 A.2d 794, 796 (1979); State v. Richards, 269 A.2d 129, 134 (1970).

A university should establish the belief (policy) that computer accounts and disk space are not immune from observation by appropriate university employees conducting tasks related to the rendition of service to the computer system and its users.

Search and Seizure in Our Electronic Society

Usually, administrators/owner have but a single relationship with those under their authority. Typically, this relationship is one of 'employer-employee.' In a University setting, there is more than one legal relationship that should be considered. A University has an 'employer-employee' relationship with its faculty and staff, but it also has a 'teacher-student' relationship with other members of its *community*. This means that there will be at least two sets of legal standards which will guide policy in this area.

The First Amendment is, for the most part, our privacy amendment. The Fourth Amendment is that which defines the circumstances under which 'privacy' can be intruded upon. So, too, will the 'privacy' area of the AUP play against the 'freedom from unreasonable search and seizure' area of the AUP. These antithetical positions force balance, and this tension will provide a sounding board to assure that the 'privacy' principles and statements in the AUP are valid and reasonable. It is an advantage when developing an AUP to craft the Search and Seizure statements in concert with the 'privacy' area as the First and Fourth Amendments are built and measured on mutual ground.[405]

---

[405] Harvey A. Silverglate and Thomas C. Viles. (1991, May). Constitutional, legal, and ethical considerations for dealing with electronic files in the age of cyberspace. Paper presented at the 1991 Federal Enforcement Conference, Georgetown University Law Center, Washington, DC. The courts recognize that the First and Fourth Amendments grew from the same historical source, for the struggle for press freedom was energized by the struggle against the license to print, and against the prior restraints imposed by the Crown to enforce the license. In the Supreme Court's words, "the struggle for the freedom of the press was primarily directed against the power of the licensor ... And the liberty of the press became initially a right to publish 'without a license what

It is important to clearly define this area in an AUP, as law enforcement agencies and the legal system have not yet provided a clear set of standards. With respect to computer searches and seizures, Kapor and Godwin state that law enforcement "lack[s] understanding, both of the new technology, and - just as important - of how it is normally used, and they simply cannot conduct the discretion-less, particular searches and seizures required by the Fourth Amendment when those searches and seizures involve computer equipment and data."[406]

What's happening is that law enforcement agencies have attempted only to discern what are misuses of a computer. This creates a situation where law enforcement agencies do not routinely recognize the First Amendment significance of BBSs and other forms of electronic speech and publishing. The resulting problem is that there is a tendency to issue broad search and seizure warrants. Warrants issued based on this line of thought can, in the long term, abridge the free exercise of one's First Amendment rights.

> On January 24, 1990, a handful of Secret Service agents, accompanied by two employees of the local telephone company, seized the equipment of a twenty year old man living with his mother in New York. From his bedroom, they seized a Commodore 128 computer, 200 floppy disks, a telephone answering machine,

---

formerly could be published only with one.'" While this freedom from previous restraint upon publication cannot be regarded as exhausting the guaranty of liberty, the prevention of that restraint was a leading purpose in the adoption of that constitutional provision. Lovell v. City of Griffin, Ga., 303 U.S. 444, 452 (1938). The Supreme Court commands that special care be taken when authorizing or reviewing a search involving any entity engaged in the publication or dissemination of ideas. "Freedom of the press" long has been interpreted broadly to protect not only newspapers publishers and pamphleteers, e.g., Lovell, Id., 303 U.S. at 452, but also motion pictures, Roaden v. Kentucky, 413 U.S. 496 (1973); Burstyn v. Wilson, 343 U.S. 495, 502 (1952); United States v. Paramount Pictures, 334 U.S. 131, 166 (1948), and even computer bulletin boards, Legi-Tech v. Keiper, 766 F.2d 728, 734-35 (1985), from prior restraints and general searches. In order to avoid prior restraints on speech, the particularity requirement of the Fourth Amendment "is to be accorded the most scrupulous exactitude when the 'things [to be seized]' are books, and the basis for their seizure is the ideas which they contain." Stanford v. State of Texas, 379 U.S. 476 (1965) reh den, 380 U.S. 926 (1965), citing Marcus v. Search Warrant of Property, 367 U.S. 717 (1961).

[406] Mitchell Kapor, and Michael Godwin. (1994). Civil liberties implications of computer searches and seizures: Some proposed guidelines for magistrates who issue search warrants [On-line].

cassette-playing radio, and all of his musical cassette tapes. Apparently, the Secret Service was searching for evidence of alleged computer crimes.

On March 1, 1990 the Secret Service raided offices of Steve Jackson Games, a small Austin start-up company which designed and manufactured fantasy role-playing books and games. The Secret Service seized the company's three computer systems, two laser printers, miscellaneous hardware, papers, back-up disks, and a single pocket calculator. The company's plans and galleys for a new role-playing game, GURPS Cyberpunk, also were seized, after an agent opined that the game was a handbook for computer crime. (The format of Steve Jackson's games is similar to that of "Dungeons and Dragons"; GURPS Cyberpunk consists of a lengthy instruction book plus general information about the game. In fact, all of the company's games consist solely of printed matter. The company was not in the business of manufacturing any software.)

On May 8, 1990, as part of Operation Sun Devil another bulletin board, called 'RIPCO', was raided. All of the equipment necessary to run the bulletin board was seized. The RIPCO board had operated since 1983, and it had accumulated extensive text files which were accessible to its 600 users. No arrests were made, nor have any charges been filed against the operators. But the board was shut down.

On February 28, 1991, following an arrest for rape and battery, the Massachusetts state and local police seized the suspect's computer equipment. The suspect reportedly operated a 650-subscriber bulletin board called 'BEN', which is described as "geared largely to a gay/leather/SAM crowd." It is not clear what the board's seizure is supposed to have accomplished, but the board is now shut down, and the identities and messages of its users are in the hands of the police.[407]

An exemplary case-in-point of the issues of privacy and search and seizure is incident involving Arnaldo Lerma.[408] Lerma, a Virginia resident, posted numerous court documents on the Internet concerning the California based Church of Scientology. "In response, the church filed a copyright infringement suit against Lerma and his Internet access provider."[409] Ultimately, federal marshals and church lawyers obtained warrants, entered his home, and removed all equipment which could be used to post information on the Internet. The federal marshals seized several

---

[407] Dibbell, Gibbs. (1990, July 24). On line and out of bounds, Village Voice, page 27; Jahnke. (1990, November 14). The cops come to Cyberspace. Boston Magazine, page 140; John Perry Barlow. (1990). Crime and puzzlement [On-line]. Available as of July 1, 1996: http://www.eff.org/pub /Publications /John_Perry_Barlow /crime_and_puzzlement.1.

[408] Nguyen Lan. (1995, Aug. 13). Virginia man's computer seized in Internet lawsuit. Washington Post, page B6.

[409] Caden and Lucas at para 12.

hundred floppy disks, a number of hard drives, a computer system and a scanner. The case against Lerma was dismissed and all seized material was returned to Lerma.[410]

These are but a few examples of the gulf between law enforcement and the Constitution in the area of computer related search and seizure issues. This gulf needs to be bridged by the establishment of practical as well as theoretically sound Search and Seizure procedures which protect the rights and responsibilities of all parties concerned. Prosecutors are well aware of the kinds of misuses to which computer technology lends itself. But that 'awareness' does not address the legal uses of computer systems. This is a major predicament, as the magistrate who must issue search warrants, and, by decendancy the System Administrator who has magistrate-like functionality in regard to the computer system, have an inadequate recognition level of what legal procedures should guide them. The magistrate must have this knowledge in order to judge whether or not a given petition for search demonstrates *probable cause* for suspicion of criminal activity.

So, too, the system administrator should be able to judge whether a given action, or situation, would legally allow a search of a user's disk space (and from that search, possibly, have a legal basis for further action). Without a set of acceptable legal standards upon which to base these decisions, the magistrate and the System Administrator lack the ability to protect the rights of users and to insure the safety and well-being of their system. Therefore, it becomes necessary to develop AUP statements to address the issue of search and seizure, especially since the line between constitutionally allowable searches and seizures and illegal searches and seizures, in respect to computers, is dim and uncertain. Establishing University policy

---

[410] Religious Technology Center v. Lerma, et. al., 95-1107-A E.D. Va. (November 29, 1995).

which speaks to these issues will aid in insulating the University from legal conflicts as well as in forestalling the workaday conflicts generated by dissatisfied users.

The Electronic Frontier Foundation (EFF) has been developing model search and seizure guidelines. The EFF hopes to persuade the American Bar Association to adopt their model in place of its current guidelines for the issuance of search warrants relating to business records. In an attempt to make searches less intrusive and destructive, Kapor and Godwin of the EFF recommend that:

> 1. computers used for publishing or electronic bulletin boards be afforded the same First Amendment protections as other means of publication;
>
> 2. in determining if just cause for seizure of equipment and software exists, judges shift the emphasis from what is technologically possible (e.g. an electronic trip wire that can erase all data) to what is likely to happen;
>
> 3. the search of computer disks take place on a business's premises, whenever possible;
>
> 4. under most circumstances, computers be seized only when they are the instruments of a crime.[411]

These guidelines seem to be excellent protection for a University, its employees, and its students. The EFF's model is an excellent balance between the user's right to privacy, and, the University's right to safeguard its systems, and other users on those systems.

Applying Fourth Amendment Protection to Cyberspace

Given the Supreme Court's approach to measuring the scope of the Fourth Amendment's protection, it is very difficult to predict what the Court will have to say

---

[411] Mitchell Kapor, and Michael Godwin. (1994). Civil liberties implications of computer searches and seizures: Some proposed guidelines for magistrates who issue search warrants [On-line].

about future cases which involve *property* which exists in cyberspace. As there is a need to strike a balance between society's need to have security and protection from crime and the individual's right to privacy, Junker[211] notes that "every fourth amendment decision chooses, at the margin, which of these opposing values to prefer, and the doctrine reflects and accommodates that choice."[412]

Sergent believes that it will be difficult to predict the legal reasoning which will be used in future cases for four reasons:

> First, Katz's objective reasonable expectation of privacy standard is not an objective standard at all. Even if applied as envisioned by its author, the test would have to balance what types of privacy we should have, how much that privacy is worth, and the strength of the law enforcement interests. In the hands of a court that consistently values crime control over individual privacy, the main function of the expectation of privacy rubric minted in Katz seems to have been to provide an additional ground for denying fourth amendment protection.
>
> [Second,] [t]he Court confuses the Katz standard even more by refusing to acknowledge that it is making a normative determination. Thus [as Junker notes], the standard is subtly reinforced ... with doctrinal and analytic devices that make it receptive to the majority's values and which undermine or deflect Katz' promise to protect any justifiable expectation of privacy.
>
> Third, when the analysis points in one direction and the Court wishes another result, the Court changes analytical tactics. For instance, when the expectation of privacy analysis provides poor support for its position, the Court returns to the textual approach that was rejected in Katz. [Junker notes that in] addition, when the actual facts seem to demand Fourth Amendment protection, the Court deflects that result by substituting proxy facts, hypothetical circumstances that appear similar to the case at hand but which carry an opposite doctrinal charge.
>
> Finally, the Court often blurs the line between the scope of the Fourth Amendment and its content, making it difficult to distinguish cases in which one discloses information, leaving no Fourth Amendment protection at all from those in which one merely grants a third party the ability to consent to a search. The Court's dislike for the exclusionary rule as a remedy leads it to limit the scope and content of the Fourth Amendment, in order to limit the amount of evidence that is excluded.[413]

---

[412] John M. Junker, The Structure of the Fourth Amendment: The Scope of the Protection, 79 J. Crim. L. & Criminology 1105, 1177(1989).

[413] Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (1995) at 1193.

Circumstances for Intrusion - Search Warrants

> When an individual has a privacy or Possessory interest in electronic data, the Fourth Amendment provides protection against unreasonable police searches or seizures. The level of this protection depends largely upon the circumstances under which the search or seizure is conducted and the underlying nature of the stored electronic information. Although the Supreme Court has asserted that a warrant is generally necessary to conduct a search, police can often act on less authority. Many of the situations in which police will not need a warrant can apply to computer data.[414]

> The informed and deliberate determinations of magistrates empowered to issue warrants as to what searches and seizures are permissible under the Constitution are to be preferred over the hurried action of officers and others who may happen to make arrests.[415]

In Johnson vs. United States, the U.S. Supreme Court established the importance of securing a search warrant when intruding upon persons, their house, papers, or effects which are otherwise protected by the Fourth Amendment to the Constitution:

> The point of the Fourth Amendment ... is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.[416]

The Johnson Court, in regard to the same point, continues to comment and states that "there are exceptional circumstances in which, on balancing the need for effective law enforcement against the right of privacy, it may be contended that a magistrate's warrant for search may be dispensed with."[417]

Johnson is an excellent example of the debate over the requirements. It illustrates that warrants tend to reduce law enforcement's discretionary ability to intrude into otherwise protected areas. The time (and possibly the expense) of obtaining a warrant might otherwise hinder law enforcement activities.

---

[414] Sergent at 1185.
[415] United States vs. Lefkowitz, 285 U.S. 452, 464 (1932).
[416] Johnson v. United States, 333 U.S. 10, 13 (1948).
[417] Johnson v. United States, 333 U.S. 10, 14-15 (1948).

In recent years the courts have been much stricter when judging the reasonableness of police actions in regard to search warrants. There are, however, a number of areas in which a search warrant is not required in order to perform a search. An analogy may be drawn between allowable automobile searches and seizures, and computer searches and seizures. The Supreme Court has allowed searches of an automobile which were for the purpose of inventorying contents,[418] where the vehicle was towed back to the police station to be searched,[419] when the search was made given simply the existence of probable cause,[420] and/or when a search was made of closed containers within car.[421]

In commenting on Acevedo, Mr. Justice Scalia wrote that "... even before today's decision the 'warrant requirement' had become so riddled with exceptions that it was basically unrecognizable."[422]

In commenting about the state of affairs of computer networks and the Fourth Amendment, Sergent says:

> Because computer information and the networks that carry it are new technologies, it may be difficult to determine how the "exceptions" to the warrant requirement would apply. Examining the policies underlying which standard of review courts apply may enable us to see how far courts will extend existing exceptions or create new ones.[423]

The key to this issue is to determine the scope of privacy on a university computer system. In other words, what 'expectation of privacy' will the user of a university's computer system have. Since Katz pronounced that the "Fourth Amendment protects people, not places", it would seem reasonable that computer spaces (not being a live person) are not afforded as much protection as we may be

---

[418] Colorado vs. Bertine, 479 U.S. 367 (1987); Illinois vs. Lafayette, 462 U.S. 640 (1983).
[419] Chambers vs. Maroney, 399 U.S. 42 (1970).
[420] Chambers vs. Maroney, 399 U.S. 42 (1970).
[421] California vs. Acevedo, 500 U.S. 565 (1991).
[422] California vs. Acevedo, 500 U.S. 565, 582 (1991).
[423] Sergent at 1207.

lead to believe. The determinations now center around protecting the individual's privacy.

A search of a user's computer space may be justified if the system management has "articulable suspicion."[424] A key element in a 'search and seizure' which is generated by "articulable suspicion"[425] is that the duration is brief.[426] The allowable scope of this type of search is justified by the suspicion of the person executing the search (and possible seizure).

Probable cause is another component of search and seizure. Probable cause exists where "the facts and circumstances within their [the officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been or is being committed."[427]

In a 1991 law review article, Stuntz surveyed the exceptions to the need for a required search warrant and concluded that "all these rules mean [is] that given

---

[424] Terry v. Ohio, 392 U.S. 1, 27 (1968). Terry defined "articulable suspicion" as "the specific reasonable inferences which [an officer] is entitled to draw from the facts in light of his experience."

[425] Terry v. Ohio, 392 U.S. 1, 27 (1968). Terry defined "articulable suspicion" as "the specific reasonable inferences which [a police officer] is entitled to draw from the facts in light of his experience."

[426] United States v. Place, 462 U.S. 696, 709-10 (1983). The court ruled an action unacceptable under the Fourth Amendment action where luggage was detained for 90 minutes and taken to another airport for a "sniff test" by a narcotics detection dog "exceeded the permissible limits of a Terry-type investigative stop." This time period, and the fact that the luggage was moved to another airport was deemed not to be of minimal duration and thus the search was illegal absent a warrant.

[427] Brinegar v. United States, 338 U.S. 160, 175-76 (1949), quoting Carroll v. United States, 267 U.S. 132, 162 (1925).

probable cause to believe that the defendant is guilty of a crime[,]... the police can search pretty much everything they want, apart from the defendant's home."[428]

Due Process: An Introduction

> "Due process," unlike some legal rules, is not a technical conception with a fixed content unrelated to time, place and circumstances. Expressing as it does in its ultimate analysis respect enforced by law for the feeling of just treatment which has been evolved through centuries of Anglo-American constitutional history and civilization, "due process" cannot be imprisoned within the treacherous limits of any formula. Representing a profound attitude of fairness between man and man, and more particularly between the individual and the government, "due process" is compounded of history, reason, the past course of decisions, and stout confidence in the strength of the democratic faith which we profess.[429]

The legal system in the United States of America is based upon the notion that regime level policy can not be contrived, enacted, and enforced without the consent of the governed. The First Continental Congress decreed: "Resolved, N.C.D. 8. That [citizens] have a right peaceably to assemble, consider of their grievances, and petition the king; and that all prosecutions, prohibitory proclamations, and commitments for the same, are illegal."[430]

Such was the position of the American colonists in regard to their right to 'due process.' The colonists believed that all things which affected their lives should follow a fair and equitable process.

To become a law, an issue should undergo free debate by legislators, followed by a vote which will cause the issue to be enacted or defeated. In a criminal proceeding, a person is charged with a crime, and then brought before a jury of his/her peers. The person and the state are represented by counsel, there is an

---

[428] William J. Stuntz, Warrants and Fourth Amendment Remedies, 77 Va. L. Rev. 881 (1991).

[429] Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 162-63 (1951) (Felix Frankfurter, J., concurring).

[430] Declaration and Resolves of the First Continental Congress, Journals of Congress (ed. 1800), I. pp. 26-30.

impartial judge, all the facts are heard, and then the jury renders its verdict. In short, if proper 'procedures' have been followed in rendering a result, that result should be acceptable. Concerning all but relatively trivial matters, a person is entitled to such 'due process.'

The first reported case involving 'due process' was Calder v. Bull[431] in 1798. The 'due process' issue in this case was that a citizen was deprived of his rights by a law which was enacted 'after the fact.' The citizen had committed an act, and then, at a later time, a law was enacted and he was subjected to prosecution for that act.

A landmark 'due process' case occurred in 1857 when the Supreme Court was faced with Dred Scott v. Sanford[432] The facts in this case set another brick in place in the foundation of substantive due process. Dred Scott was a slave who had fled from his owner in a slave state to Illinois (a 'free' state). It was Mr. Scott's hope that this action would cause him to be a free person. Dred Scott sued his owner, arguing that, by virtue of being in a free state, he himself was free. The Supreme Court decided against Mr. Scott. In its ruling, the Court invalidated the Missouri Compromise as it deprived the slave owners of their property without due process.

As a result of the aforementioned cases, the 'due process' clause of the Fourteenth Amendment[433] came to be clearly understood. *Due Process* means

---

[431] Calder v. Bull, 3 U.S. 386 (1798).

[432] Dred Scott v. Sanford, 60 U.S. 393 (1857).

[433] U.S. Const. amend. XIV. §1. "All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of right to life, liberty, or

procedure. It means *the procedure* by which a superior court could strike down the decision of a lower court if the lower court failed to follow proper procedures. Due process means that a person cannot "be deprived of life, liberty, or property without"[434] some sort of established, fundamentally fair, and equitable procedure.

Due process also requires that there be, at a minimum, some reasonable form of notice given to the person involved in the proposed action (barring exigent circumstances). The person at whom the notice is directed should have a fair opportunity to be heard on the matter.[435] Certainly this requirement varies greatly depending upon the factual content of the situation/issue. In Goldberg v. Kelley, the Supreme Court held that the extent to which procedural due process must be afforded a person is influenced by the extent to which he may be:

> condemned to suffer grievous loss … and depends upon whether the [person's] interest in avoiding that loss outweighs the governmental interest in summary adjudication. Accordingly … 'consideration of what procedures due process may require under any given set of circumstances must begin with a determination of the precise nature of the government function involved as well as of the private interest that has been affected by governmental action.'[436]

The constitution itself adjusts with changing jurisprudential values, thus, 'due process' of law does not have a fixed meaning. Justice Frankfurter stated:

> The requirement of 'due process' is not a fair-weather or timid assurance. It must be respected in periods of calm and in times of trouble; it protects aliens as well as

---

property, WITHOUT DUE PROCESS of law; nor deny to any person within its jurisdiction the equal protection of the laws" [emphasis added].

[434] U.S. Const. amend. V. "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, WITHOUT DUE PROCESS of laws nor shall private property be taken for public use, without just compensation" [emphasis added].

[435] Roviaro v. United States, 353 U.S. 53 (1957); Kwong Hai Chew v. Colding, 344 U.S. 590 (1953); Willner v. Committee on Character and Fitness, 373 U.S. 96 (1963); in re Ruffalo, 390 U.S. 544 (1968); Walker v. City of Hutchinson, 352 U.S. 112 (1956); Joint Anti-Fascist Refugee Committee v. McGrath, 341 U.S. 123 (1951); Bailey v. Richardson, 341 U.S. 918 (1951); Rosenberg v. United States, 346 U.S. 273 (1953).

[436] Goldberg v. Kelley, 397 U.S. 254, 262-263 (1970).

> citizens. But 'due process,' unlike some legal rules, is not a technical conception with a fixed content unrelated to time, place and circumstances. Expressing as it does in its ultimate analysis respect enforced by law for that feeling of just treatment which has been evolved through centuries of Anglo-American constitutional history and civilization, 'due process' cannot be imprisoned within the treacherous limits of any formula. Representing a profound attitude of fairness between man and man, and more particularly between the individual and government, 'due process' is compounded of history, reason, the past course of decisions, and stout confidence in the strength of the democratic faith which we profess. Due process is not a mechanical instrument. It is not a yardstick ... It is a delicate process of adjustment inescapably involving the exercise of judgment by those whom the Constitution entrusted with the unfolding of the process.[437]

Due Process In Regard to a Computer System

> A fundamental requirement of due process is "the opportunity to be heard" ... It is an opportunity which must be granted at a meaningful time and in a meaningful manner.[438]

The collection and dissemination of information via computer networks has been moving forward as no other creation in the history of mankind. There is an ever-growing desire for information about people, events, happenings, etc. Computers have made all sorts of information about all sorts of things readily available in all sorts of places. Severe problems can arise concerning this accumulation of information as the individual, invariably, has next to no control over its dissemination, use, and more importantly, its accuracy. Chlapowski states that: "[o]ver time, information may easily become misinformation because individuals cannot control, and thus cannot correct, the information that is disseminated."[439]

Speaking in regard to information, privacy, and computer networks, Gerety supports this contention when he states that:

---

[437] Joint Anti-Fascist Refugee Committee v. McGrath, Anti-Soviet Friendship v. McGrath, International Workers Order v. McGrath, 341 U.S. 123, 162-163 (1951).

[438] Armstrong v. Manzo, 380 U.S. 545, 552 (1965) (Potter Stewart, J.).

[439] Francis S. Chlapowski, Note: The Constitutional Protection of Information Privacy, 71 B.U. L. Rev. 133 (1991).

> [T]here is the possibility that [the information's] contents will be divulged without [the individual's] consent or knowledge and so without [the individual's] corrections ... This comes ... to a kind of institutionalized gossip, and its vice is its tendency to distortion and incompleteness, tempting others to make decisions about us, as gossips will, behind our backs and on uncertain grounds.[440]

Furthermore, it is highly possible the data which is factually accurate may be disseminated inappropriately. Chlapowski notes that "personal facts which do not become distorted may be of such a highly sensitive and personal nature that, although correct, they are potentially harmful and embarrassing if disseminated carelessly."[441] The general public needs to have protection in the event that information about them, regardless of whether true or false, is unnecessarily collected, or, inappropriately or unnecessarily disclosed.

The difficulty with challenging data collection is that such action is not usually an invasion of privacy (a legal tort). The 'reasonableness' requirement of the invasion of privacy tort limits its application in this circumstance.

> As long as the government can articulate an arguably legitimate reason for collection or disclosure, the collection will probably be considered reasonable under the common law. Often the reasons articulated for collection or disclosure are deemed legitimate, however, only because they are evaluated from the perspective of the majority—those who chose the representative government and to whom elected representatives feel most responsible. Thus, individuals who desire to keep certain personal information private are denied governmental protection of their privacy interest when the interest conflicts with the interests of the majority. In order to safeguard the privacy of these individuals, there must be a check on governmental disclosure of personal information—a mechanism to balance the interests of the individual and the interests of the government when those interests conflict.[442]

---

[440] Gerety, Redefining Privacy, 12 Harv. C.R.-C.L. L. Rev. 233, 287 (1977).
[441] Chlapowski at 134.
[442] Chlapowski at 134-35.

Due to the low standard for assurance that violation of the rights of an individual do not occur when information is collected, there should be a balance built into an AUP to insure fairness - to insure that there is a balance between the individual's interests and the university's interest. The university should deal with the concept of 'information privacy' in its AUPs 'due process' statement, or should clearly specify a 'due process' philosophy in its AUP.

Substantive Due Process

> The constitutional safe-guard of substantive due process requires that all legislation be in furtherance of a legitimate governmental objective.[443]

Information, given the age of the computer, has become a commodity - and commodities are 'property.' Assuming that this intangible computer data can be reasonably be viewed as 'property,' computer data (being 'property') is protected by the statutes that protect and safeguard the liberty and property rights of an individual. The due process clauses of the Fourth and Fourteenth Amendments safeguard both substantive *and* procedural due process.[444]

The scope of the due process clauses as they apply to a person's liberty have varied over the years as a result of a number of Supreme Court decisions. Such has not been true for the Court's interpretation of 'due process' as it applies to 'property.'

---

[443] Steven Gifis. (1991). Law Dictionary. New York: Barron's, page 56.

[444] Whitney v. California, 274 U.S. 357, 373 (1927) (Brandeis, J., concurring). This opinion states that "it is settled that the due process clause of the Fourteenth Amendment applies to matters of substantive law as well as to matters of procedure"); see also Laurence Tribe. (1988). American constitutional law (2d ed.). Mineola, NY: Foundation Press, page 769.

The Lochner Era

The *Lochner Era* derives its name from a 1905 case (Lochner v. New York[445]) in which the Supreme Court struck down many economic and non-economic laws based upon very broad concepts of liberty.

After the Civil War, the Supreme Court began to interpret 'liberty' (as in the due process clauses) more broadly than before.[446]

As Chlapowski notes:

> The Lochner-era judiciary has been criticized for extending constitutional protection to the realm of economic affairs, thus assuming a role thought to be legislative rather than judicial. This criticism of Lochner implies that the Court usurps the legislature by subjecting economic laws to scrutiny in the absence of a clear constitutional prohibition.[447]

The political and economic forces which were born out of the Great Depression of the 1930s caused the eventual erosion and eventual downfall of Lochner. Roosevelt's *New Deal* legislation was in direct conflict with Lochner dogma. In 1934, Nebbia v. New York[448] began a trend of decisions that eventually

---

[445] Lochner v. New York, 198 U.S. 45 (1905). The Court invalidated the maximum hours provision for bakers on the theory that it violated the bakers' liberty of contract.

[446] See, e.g., Allgeyer v. Louisiana, 165 U.S. 578, 589-91 (1897). The Court invalidated a state law that prohibited insurance companies which did not comply with state regulations from selling policies to persons on property within the state and from selling policies to state residents, reasoning that the law unconstitutionally interfered with liberty of contract.

[447] Chlapowski at 136.

[448] Nebbia v. New York, 291 U.S. 502, 537-39 (1934). The Court upheld a New York Milk Board price-fixing statute as neither arbitrary nor discriminatory and "reasonably deemed to promote public welfare."

lead to the 1949 Lincoln Federal Labor Union v. Northwestern Iron & Metal[449] decision which explicitly rejected Lochner.

From Lincoln Fed. Labor Union on, the Supreme Court became "reluctant to use substantive due process analysis to invalidate non-economic regulations, or at least reluctant to describe its reasoning as substantive due process analysis."[450]

Chlapwoski contends that the due process clauses of the Fourth and Fourteenth Amendments apply:

> when an individual's interests conflict with the majority's interests, a constitutional dilemma arises. If the government, in its exercise of majoritarian values, infringes upon the interests of any individual or minority group of individuals by controlling an aspect of their personal lives, the constitutional guarantee of liberty may be invoked to protect their interests from the tyranny of the majority. The Court's function is to decide which interests the Constitution protects.[451]

So, too, should a university's AUP establish and maintain a balance between the reasonably expected rights of the user and the rights of the management to insure that its systems function efficiently and properly.

A Review of Existing Acceptable Use Policies

> If we had a reliable way to label our toys good and bad, it would be easy to regulate technology wisely. But we can rarely see far enough ahead to know which road leads to damnation. Whoever concerns himself with big technology, either to push it forward or to stop it, is gambling in human lives.[452]

---

[449] Lincoln Fed. Labor Union v. Northwestern Iron & Metal Co., 335 U.S. 525, 535-37 (1949). The Court stated that Nebbia introduced the Court's "reject[ion of] the due process philosophy enunciated in the [Lochner] line of cases."

[450] Lincoln Fed. Labor Union at 538.

[451] Lincoln Fed. Labor Union at 539.

[452] Freeman Dyson. (1979). Disturbing the Universe. New York: Harper and Row, part 1, chap. 1.

Introduction

To this point, the dissertation has attempted to build a basis of wisdom from which will flow Acceptable Use Policy documents. Previously, AUP's tended to be developed by those who believed that they were mechanical-operational policies. AUP's developed in this manner were more like auditing tools or car owner's manuals. There should be a shift in the paradigm to include the issues which have been addressed in the previous pages (e.g., privacy, search and seizure, due process) and issues which will be suggested in the following pages (e.g., managing shared resources, solving social dilemmas). At this point, this dissertation will review existing AUP statements, and hopefully, the reader will apply the concepts from the previous pages.

When reading these AUP statements, one should not assume that any or all of the following statements/principles need to be part of a University's AUP. Based upon the components a University wishes to have in its AUP, some of the following statements may be appropriate—some may not be.

The statements/principles which follow appear to be the most effective in that they legally, and, fairly clearly state their intent.

Review of Selected Acceptable Use Policy Statements

> Public policy is in its nature so uncertain and fluctuating, varying with the habits and fashion of the day, with the growth of commerce and the usages of trade, that it is difficult to determine its limits with any degree of exactness. It has never been defined by the courts, but has been left loose and free of definition, in the same manner as fraud. This rule may, however, be safely laid down, that whenever any contract conflicts with the morals of the time, and contravenes any established interest of society, it is void, as being against public policy.[453]

---

[453] William W. Story. (1847). A Treatise on the Law of Contracts (2nd ed.). City: Publisher, pp. 480-81.

Acceptable Use Policy is presently generated in two basic forms: dictatorial and democratic.

- **dictatorial**

Many of the first AUPs are a list of *do* and *don't* statements - in the style of the *Ten Commandments*. The term *dictatorial* was not viewed as especially negative. Users 'back then' were comfortable with knowing what the system administration had set down as the rules. They did not disagree with these dictatorial rules, as they acceded with them.

The computer network was the *center of the universe* for many early users. But as the population of computer network users grew (see Figures 1 and 2), not all the new comers were comfortable with *the rules*.

Today most AUPs which are in force can be identified as *dictatorial*.

In short, the *dictatorial* AUP will state what the user will *do* and what will *not do*, and what will happen to the user for violation. Very few AUPs developed in this manner had any sense of the basic rights of the individual (e.g., due process, privacy).

- **democratic**

The new wave of AUPs can be categorized as *democratic*. Generally this means that the system administrators have stated what they will do in regard to a user's behavior, and, have also stated what the user's rights are. The democratic AUP creates a balance between a user's expected right to privacy, due process, freedom from unreasonable search and seizure, and the administration's right to insure the continued operation of its systems.

While reading the following selected statements[454] from existing AUP's, bear in mind that virtually all existing AUP's were crafted in a time where the document was, due to the nature and capability of the network, metaphorically like a 'Chevrolet Owner's Manual.' This was due to the fact that the computer user only needed to be aware of the mechanical and operational aspects of the network. Today, there is a need for the AUP to address the societal needs of the user. Virtually all AUPs surveyed appeared to be in the formative stages of dealing with societal needs of the user. AUP statements are attempting to address social issues (e.g., privacy, harassment, due process), but the statements tend to be vague and overly broad. Dealing with the societal needs of the user is a non-trivial change in the drafting of AUP's. This change is a radical adjustment in the existing paradigm which drives AUP construction. The development of an AUP should shift paradigms to also address community issues that are now inherent on computer networks. The AUP should now be a social contract in addition to being the 'owners manual.'

The following AUP's are reflective of existing documents.

The Ohio State University[455]

The AUP states:

> It is recognized that computer files are a new form of property separable from the media with which they are recorded, and that close analogies can be found between the uses of computer files and of various other forms of physical property. The Department shall use these analogies in making decisions about the appropriate use of computer files and the protection of their privacy, extending as nearly as possible exactly the same protection to computer files as is traditionally extended to the analogous physical property.
>
> The spirit of this policy is that the file space provided by the University to individuals has exactly the same status as analogous, more tangible facilities also provided by the University. Such facilities as private library carrels, dormitory

---

[454] This study surveyed a large number of AUP's and selected those which seemed to be typical of those available.

[455] Ohio State University AUP [Online]. Available as of July 1, 1996: gopher:// gopher.eff.org /11/CAF/policies.

> rooms, and gym lockers are technically owned by OSU, and may be entered only for "administrative" purposes such as building maintenance. Similarly, the computers and computer files of students, staff, and faculty members, being electronic extensions of their personal work areas, may not be inspected, copied, changed, or otherwise tampered with without the permission of the owner, except for purposes relevant to the administration of the computer system. Notice that copying (i.e., stealing or "pirating") computer software is also prohibited under this policy.

Ohio State has done an excellent job in defining how they view the computer system. It provides helpful guidance to users of its systems and is not at all authoritarian. Users who violate this policy would be hard pressed to argue that they did not understand what they were doing was wrong, as OSU has provided both policy and education about the policy.

The only criticism of the OSU AUP is that it makes vague comments about which analogies apply to "physical property." This vagueness, however, seems to be due to a vagueness in legal precedent. The policy appears to be workable as such vagueness may need to be clarified by the courts before Universities can follow suit. It may also be in the University's best interest to leave this intentionally vague so that issues can be handled on a case by case basis.

McGill University, Montreal, Canada[456]

The AUP states:

> Within the Department of Electrical Engineering, personal files, including files stored on computer, electronic mail, and other electronic communications are to be considered private.

This is a very straight forward statement which clearly states what McGill intended to say. It is, nevertheless, a bit too brief. It establishes that privacy exists and is applicable to the computer system and its contents. But McGill is overly broad in its pronouncement. Taken as read, NetNews would also fall into the same category

---

[456] McGill University AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org /11/CAF/policies.

as does 'files stored on the computer system [and] electronic mail.' Such is not the case, NetNews is public, and, electronic mail is private.

Michigan State University[457]

The AUP states:

> Staff should at all times respect the privacy of user files, mail, and printer listings

On the real campus, it seems to go without saying that 'staff should . . . respect the privacy of' the students and other staff members. But in cyberspace, that notion needs to be repeated quite often, as the concept is not yet ingrained in us.

This AUP does not actually seem to say anything that can be enforced. They essentially ask staff members to be courteous to others. While this is a positive goal, it is far too vague and unenforceable.

University of Illinois at Urbana-Champaign[458]

The AUP states:

> Network and system administrators are expected to treat the contents of electronic files as private and confidential. Any inspection of electronic files, and any action based upon such inspection, will be governed by all applicable U. S. and Illinois laws and by University policies.

UI's policy is clear and well stated. This policy statement is on a par with that of Ohio State University's AUP. However, given a lack of appreciation of the nature of cyberspace which the typical user has, it would be advantageous for the University of Illinois to provide some educational wording so that the user could better understand 'the rules.'

---

[457] Michigan State University AUP [On-line]. Available as of July 1, 996: gopher:// gopher.eff.org/11/CAF/policies.

[458] University of Illinois-Urbana Champagne AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

Dalhousie University[459]

The AUP states:

> Nothing in this Guide diminishes the responsibility of system administrators of computing services to take remedial action in the case of possible abuse of computing privileges. To this end, the system administrators with the approval of the President and with due regard for the right of privacy of users and the confidentiality of their data, have the right, to suspend or modify computer access privileges, examine files, passwords, accounting information, printouts, tapes, and any other material which may aid in an investigation of possible abuse. Whenever possible, the cooperation and agreement of the user will be sought in advance. Users are expected to cooperate in such investigations when requested. Failure to do so may be grounds for cancellation of computer access privileges.

Dalhousie University has crafted a number of poor statements in their AUP. It is uncertain about Canadian law, but if this AUP were implemented in the USA, it would tread on several Constitutional rights. The AUP indicates that due process is to be followed, but the authoritarian tone of this statement leads one to believe otherwise.

Also this AUP requires computer users to cooperate in investigations. While this is a fine notion, "failing to cooperate" is a vague concept. It is also worth noting that "[f]ailure [to cooperate] ... may be grounds for cancellation of computer access privileges", seemingly, without due process.

James Madison University[460]

The AUP states:

> Students, faculty and staff who use the computer have the right to privacy and security of their computer programs and data. Computer users should not tamper with files or information that belongs to other users or to the operating system.

James Madison has a fairly good AUP. The only criticism is that the statements seem skewed toward the user's rights and responsibilities and do not

---

[459] Dalhousie University AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org /11/CAF/policies.

[460] James Madison University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org /11/CAF/policies.

provide the same clarity in respect to the administration's rights and responsibilities. More needs to be said about what the administration can and can do.

University of California at Berkeley[461]

The AUP states:

> Privacy - Individuals' rights of privacy shall not be violated without reasonable cause.

This is a sound general statement. It might be an very good opening sentence in a paragraph. But it surely cannot be left to stand unclarified.

University of Michigan[462]

The AUP states:

> The University characterizes as unethical and unacceptable, and just cause for taking disciplinary action up to and including non-reappointment, discharge, dismissal, and/or legal action, any activity through which an individual:
> [. . .]
> (e) without authorization invades the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources,

AUPs should refrain from setting an authoritarian tone. As the overwhelming number of users on a system will be virtual novices, is best to adopt an educational rather than an authoritarian posture.

The AUP leads one to believe that a casual intrusion of another's privacy (not that this is acceptable) could lead one to be dismissed from the University. While this may be true as a practical matter, stating it here sets an unwanted tone for an AUP. It is even more of a problem since 'privacy' itself is not generally well defined in regard to computer systems. Charging a person with a violation of policy where the act is not defined seems to be a conundrum.

---

[461] University of California at Berkeley AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

[462] University of Michigan AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

> This policy is applicable to any member of the University community, whether at the University or elsewhere, and refers to all information resources whether individually controlled, or shared, stand alone or networked.

It may not be judicious to lump University employees and students into the same legal kettle. A University has an employer-employee relationship with its faculty and staff which is legally different than its relationship with the students.

New Mexico State University[463]

The AUP states:

> All computer users have two basic rights--privacy and a fair share of resources.

This statement, and the one which follows, are included to show how concise a statement can be. Granted it may be too concise, but it does impart two ideas (aside from 'privacy' and 'fair share of resources'). The user is given the sense that the University is concerned with their rights, and the rights of others.

University of Pittsburgh[464]

The AUP states:

> Every member of the University of Pittsburgh has two basic rights regarding computing--privacy and a fair share of resources.

This statement, while supporting privacy and a fair share of the computing resources, is unworkably vague and overbroad. The is also no explanation of what privacy means. Nor is it clear as to what a fair share of the computing resources means.

---

[463] New Mexico State University AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

[464] University of Pittsburgh AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

Washington University[465]

The AUP states:

> **Privacy**
>
> All user accounts are considered the private domain of the user who owns them. All users should expect that, regardless of the protections set on their files, they will not be read by others. System Management personnel will only view users' files under exceptional circumstances.

This statement seems to assume a level of expertise which the typical user does not initially possess. What percentage of users are aware of 'file permissions', let alone how to set them. Given the level of knowledge of the typical user, it can *NOT* be argued that a violator 'knew, or *should have known*' that what they were doing was wrong..

It is also questionable whether the University should turn ownership of a computer account over to the user. A different legal standard is applied to those who 'own' property as opposed to those who are given access to the property of another.

University of New Mexico[466]

The AUP states:

> UNM recognizes that files and mail messages are confidential. Appropriate UNM employees may access computer users' files during normal maintenance and will report unlawful activities to the proper authorities.

The University of New Mexico categorizes mail messages and user files as 'confidential.' It is not clear what this term means. It is not clear if 'confidential' equates to 'private', or refers to some lesser degree of seclusion. But the concept of 'confidential' does enable UNM employees to access the user's account and snoop about without any cause.

---

[465] Washington University AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

[466] University of New Mexico AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

Purdue University[467]

The AUP states:

> Don't inspect private user files and mailboxes unless the administration of a Computing Center system requires it.

This statement is unenforcably vague. It does indicate who can 'inspect private user files and mailboxes.' Also, simply because the administration 'requires' inspection of a user's account, that does not make it legal.

Kansas State University[468]

The AUP states:

> The third category is access to another user's account and/or files or electronic mail for the purpose of invading an individual's privacy. This is considered breach of privacy and is prosecutable under Kansas law.

This is a poor statement and does not seem to have an actual basis in law. Privacy, as Constitutionally defined, is not tied to a place. It is a personal right. There may be an interpretation in the future which embodies specific places with privacy rights, But such does not exist today. This AUP seems to contend, or intentionally lead one to believe, that laws and decisions mean other than what they state.

Electronic Frontier Foundation[469]

Note: This document is based, in part, upon policies of the American Library Association and the American Civil Liberties Union.

The AUP states:

> The principles of academic freedom apply to academic computer systems. Computer polices should be consistent with general university codes and widely

---

[467] Purdue University AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org /11/CAF/policies.

[468] Kansas State University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

[469] Electronic Freedom Foundation AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

accepted statements on academic freedom such as the Joint Statement on Rights and Freedoms of Students.

Interpretation: "Academic institutions exist for the transmission of knowledge, the pursuit of truth, the development of students, and the general well-being of society. Free inquiry and free expression are indispensable to the attainment of these goals. As members of the academic community, students should be encouraged to develop the capacity for critical judgment and to engage in a sustained and independent search for truth."

Principle: The principles of intellectual freedom developed by libraries should be applied to the administration of information material on computers. These principles are explained in such American Library Association documents as the Library Bill of Rights, the Freedom to Read Statement, and the Intellectual Freedom Statement.

Interpretation: Computer sites that offer newsgroups should select newsgroups the way that traditional libraries select magazines and books.

Interpretation: "Every [academic computer] system should have a comprehensive policy on the selection of [information] materials." (ALA Workbook for Selection Policy Writing.

Interpretation: "Materials should not be proscribed or removed because of partisan or doctrinal disapproval" (Article 2, Library Bill of Rights).

Principle: The principles of academic freedom applicable to student and faculty publication in traditional media, apply to student and faculty publication in computer media.

Interpretation: An article or note posted by a student to a newsgroup is a student publication.

Interpretation: "Student publications [and the publications of other users] are a valuable aid in establishing and maintaining an atmosphere of free and responsible discussion and of intellectual exploration on the campus. They are a means of bringing [. . .] concerns to the attention of the faculty and the institutional authorities and of formulating [. . .] opinion on various issues on the campus and in the world at large."

Interpretation: "The institutional control of campus facilities should not be used as a device of censorship." "[User publications] should be free of censorship and advance approval of copy . . ."

Interpretation: "All university published and financed [user] publications should explicitly state [. . .] that the opinions there expressed are not necessarily those of the college, university, or student body.

The EFF has provided policy statements, education as to the reasons behind each statement, interpretations of the policy statements, and they cite many time

honored customs of organizations who have similar policies (such as the American Library Association, and the ACLU). This is unmistakably an excellent creation. It provides a balance between the rights and responsibilities, of the users, and, of the system administrators.

One caveat is worth noting here. The American Library Association has done an excellent job creating and refining their policies (which are cloned into EFF's policies). Many of these policies give rise to understanding what policies need to be in place on a computer system. However, we should always realize that ALA's policies are aimed at books. Books are inanimate objects—they are lifeless. NetNews is somewhat analogous to books and as such ALA policy may be metaphorically applicable to a certain degree. On the whole however NetNews is not an inanimate object - it has a human being attached to it in a manner of speaking - a book does not have this link. Setting policy for NetNews based upon 'books' may have pitfalls in the long term.

A review of quite a number of AUPs did not seem to reveal 'one best AUP' that all universities might adopt. There are a number of university AUPs which have specific policy statements that are well crafted and bear review. The statements that have been included here should provide a sound foundation for developing the basic philosophy for a University's AUP.

While the previous section of this paper dealt with general philosophies and components of selected AUPs, the next section will pose specific AUP statements.

Poor Privacy Protection

What qualifies these as the 'Poor' statements is that they do not:

1. consider the human condition and/or the capabilities of computer system,
2. conform with federal statutes and/or campus policy,

3. state their intent clearly and unambiguously, and,

4. account (when appropriate) for the social nature of the network.

Boston University[470]

The AUP states:

> Boston University reserves the rights to: limit or restrict any account holder's usage, inspect, copy, remove or otherwise alter any data, file, or system resources which may undermine the authorized use of that system with or without notice to the user. The University also reserves the right to periodically check the system and any other rights necessary to protect the University computer facilities.

While the AUP appears to protect the privacy of users and the integrity of the system,[471] this policy attacks privacy. It inflicts speech restrictions that would be ridiculed if applied to the campus as a whole. It is vague, and seemingly illegal[472] when it indicates that a user may not "make accessible offensive [or] annoying material."[473]

Professor Carl Kadie of the University of Illinois imagines what an uproar there would be if this policy were generalized to the University as he notes below:

- The University has the power to, without notice, inspect any assigned office space or dorm room.
- Members of the University community may NOT distribute or make accessible offensive or annoying material.
- Members of the University community may be punished for infractions against rules that are NOT listed here.

---

[470] Boston University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org /11/CAF/policies.

[471] Boston University AUP [Online]. Available as of July 1, 1996: gopher:// gopher.eff.org /11 /CAF/policies. This document states: "The University disclaims responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of the University's computer facilities."

[472] Brandenberg v. Ohio, 395 U.S. 444 (1969) is a decision which expressed the view that there was no right to speech that advocated violence. Thus, the Supreme Court's standard is that speech may not be suppressed or punished unless it is intended to produce "imminent lawless action" and it is "likely to produce such action."

[473] Boston University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org /11/CAF/policies.

- Members of the University community must not "misuse University property," where "misusing University property" is defined as misusing University property.

- The University has the power to "amend the Conditions and Policies at any time without prior notice."[474]

Poor Freedom of Speech and Privacy Protection

University of Texas[475]

The AUP states:

> Users of electronic mail and bulletin boards should avoid sending messages that are libelous, patently offensive, or that intimidate, threaten, demean, or harass individuals or groups, or that would otherwise bring discredit to the University or the Department.

This policy is somewhat better than most, but due process procedures should be detailed, privacy should be better protected, and unconstitutional speech restrictions should not be imposed. In these three areas, the policy is overly broad.

1. The procedure for computer expulsion should be detailed. It is not clearly defined who decides to apply expulsions, how a punishment/judgment might be appealed, or how a formal hearing is requested.
2. The Texas AUP also requires users to acknowledge the policy statements by a signing a release form which authorizes the University to "examine the user's files if required as part of their official duties." Mandating that a user sign a statement does not make an unreasonable search reasonable, or legal.

---

[474] Dr. Carl Kadie (personal e-mail, May 20, 1994).

[475] University of Texas AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org /11/CAF/policies.

3. This AUP is vague. It does not define who authorizes a search or determines the reasons for it, and it fails to indicate if the user is notified before or after the search.[476]

This AUP goes on to state that "[u]sers of electronic mail and bulletin boards should avoid sending messages that are libelous, patently offensive, or that intimidate, threaten, demean, or harass individuals or groups, or that would otherwise bring discredit to the University or the Department."[477] This rule likely violates United States law (Brandenberg v. Ohio[478]). Most offensive speech, demeaning speech, and speech that brings discredit to the department is protected by academic freedom and the Constitution. The rule likely also violates the University's general policy on freedom of expression.

---

[476] David Rubin. (1984). The Rights of Teachers: The Basic ACLU Guide to Teacher's Constitutional Rights. New York: Bantam Books, page 92. It states that there are legal limits to what a (public) school can ask its teachers to sign. [Some of these same limits might apply to what a school can ask a user to sign as a condition of getting (or keeping) a computer account.]; Gillard vs. Schmidt, 579 F.2d 828 (1978) is a court ruling that the school board could not search the desk of a school counselor without a search warrant. A School guidance counselor sued a school board member under civil rights statute alleging violation of his Fourth Amendment rights to be free from unreasonable government intrusion. The United States District Court for the District of New Jersey, at Newark, Lawrence A. Whipple, J., dismissed the complaint, and plaintiff appealed. The Court of Appeals, Rosenn, Circuit Judge, held that: (1) the action of school board member in searching the school guidance counselor's desk during evening, having gained access to locked counselor's suite by aid of janitor with passkey, in search of identity of person who had drawn cartoon ridiculing financial and personnel policies of school board constituted a Fourth Amendment violation, and (2) the search was an action under color of state law within meaning of civil rights statute; United States v. Nasser, 476 F.2d 1111, 1123 (1973). The Internal Revenue Service of the US searched an employee's office to determine the employee's proper performance at work. United States v. Hagarty, 388 F.2d 713 (1968). This case involved the search of a government employee's office to secure criminal evidence against him was held to violate the Fourth Amendment.

[477] University of Texas AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org /11/CAF/policies.

[478] Brandenberg vs. Ohio, 395 U.S. 444 (1969) is a decision which expressed the view that there was no right to speech that advocated violence. Thus, the Supreme Court's standard is that speech may not be suppressed or punished unless it is intended to produce "imminent lawless action" and it is "likely to produce such action."

Poor Due Process, Privacy, Freedom of Expression Protection

University of Hawaii at Manoa[479]

The AUP states:

> Those who cannot fulfill their responsibilities as users of a multiuser system will have their accounts suspended or terminated, thus it is essential that you understand what is expected of you. Please remember that an account on Wiliki is a privilege granted to you as a student, faculty, or staff member in the College of Engineering, not a right, and its continued use is dependent upon responsible behavior on the part of you, the user.

Several parts of the policy seemingly violate legal and moral requirements for due process, privacy, free expression, and user participation.

The policy asserts, several times, that computer use is a privilege not a right. This has been held to be a "wooden argument"[480] as privileges and rights are often Constitutionally the same. Even if you believe that computer usage is not a right, certainly 'due process' is.

In Goss v. Lopez, the Supreme Court said a "student's legitimate entitlement to a public education is a property interest which is protected by the Due Process Clause and . . . may not be taken away for misconduct without adherence to the minimum procedures required by that Clause."[481]

The Court went on to say that "the Due Process Clause also forbids arbitrary deprivations of liberty. 'Where a person's good name, reputation, honor or integrity is at stake because of what the government is doing to him,' the minimal requirements of the Clause must be satisfied."[482]

---

[479] University of Hawaii at Manoa AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

[480] Board of Regents v. Roth, 408 U.S. 564 (1972) states that in "most cases U.S. courts no longer recognize the wooden distinction between privileges and rights."

[481] Goss v. Lopez, 419 U.S. 565 (1975), 42 L.Ed.2d. 725, 95 S.Ct. 729.

[482] Goss v. Lopez, at 582.

This policy allows the system administrator to summarily suspend a user's access before anything has been proven, and even, before 'due process' is begun.

The system administrator is allowed to search a user's mail box and other account space at his/her own discretion. This seems to violate the ECPA bar against warrantless snooping.

Mankato State University[483]

The AUP states:

> The faculty/staff of the University reserves the right to examine files and accounting system information generated through student use of the University computing facilities."
>
> Academic computing resources on the Mankato State University Campus are for use in the instructional, research, and outreach activities of the University only.

One comment suggests that part of the policy is "so vague as to be unenforceable. . ." Other critiques say: "These statements lead me to believe that the philosophy behind the policy is that students are only allowed to use the computers for *specific* class projects . . . students may not send e-mail, read news, write programs other than those assigned, experiment with the OS or languages, use word processors except as required for the assignments. Also *anyone* can search my account!"

As applies to "using userids to play games or send messages to another," David Zuhn (zoo@cygnus.com) remarks "What? I can't send mail? Or use talk(1)? This is so vague as to be unenforceable, I'd imagine."

---

[483] Mankato State University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

This policy also states that:

> academic computing resources on the Mankato State University Campus are for use in the instructional, research, and outreach activities of the University only. Student users are authorized use of the resources only under their own userids, and only for those purposes authorized by their instructor or projects under which they have authorized access.

Dan Zabetakis contends that:

> these statements lead me to believe that the philosophy behind the policy is that students are only allowed to use the computers for *specific* class projects. In other words, an instructor will say 'write a program that does _____', and the class will use the machines to compose and debug their assignments, and for no other purpose.

Generally the Mankato policy is good but there are several severely flawed statements that need revision.

Poor Netnews Policy

Iowa State University[484]

The AUP states:

> While most of these newsgroups provide a wealth of technical, research-based, and collateral material, a few groups may contain material whose use may be illegal under state or federal law, e.g., laws governing child pornography or sexual harassment statutes governing hostile environments.

Carl Kadie notes "that The Iowa State University policy should better reflect intellectual freedom by more accurately reflecting library policy (and the law)."[485] The AUP also bans newsgroups as they "may be illegal"[486] under state or federal law. These kinds of comments indicate a lack of knowledge of existing law.

According to this NetNews AUP, users are limited as to what newsgroups they can access. It would seem that a requirement for a person to sign a form in order to have access to controversial newsgroups is a violation of the Library Bill of Rights.

---

[484] Iowa State University AUP: Critique [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies/iowa_state_critique.

[485] Iowa State University AUP: Critique [On-line].

[486] Iowa State University AUP Critique [On-line.

The U.S. Supreme Court in Island Trees Union Free School District v. Pico, 457 U.S. 853, 866-67. has recognized that:

> the right to receive ideas follows ineluctably from the sender's First Amendment right to send them ... More importantly, the right to receive ideas is a necessary predicate to the recipient's meaningful exercise of his own rights such as speech, press, and political freedom.

Apparently this AUP regards the electronic forums which are created at Iowa State University as the sole property of the University and appears to liken them to a very private office space. Carl Kadie notes that the "Supreme Court calls created forums, such as a student newspaper or campus mail systems, *limited public forums*." The Court states that the government can limit who may access these forums and/or what topics may be discussed. But otherwise, it is bound by the same standards as apply in a traditional public forum...content-based prohibition should be narrowly drawn to effectuate a compelling state interest.

Best Privacy Protection Statements

What qualifies these as the *Best* statements is that they:

1. consider the human condition and/or the capabilities of computer system,
2. conform to federal statutes and/or campus policy,
3. state their intent in a clear and unambiguous way, and,
4. account (when appropriate) for the social nature of the network.

Many of the following AUP statements are cited here without comment. This should be interpreted to mean that those statements are fulfill the above criterion. While there is great room for improvement in most of these statements, they are the best existing statements. These best statements are generally breaking new ground—

they address the issue of the need for social-legal constructs in the development of AUP's.

University of Illinois at Urbana-Champaign[487]

The AUP states:

> Network and system administrators are expected to treat the contents of electronic files as private and confidential. Any inspection of electronic files, and any action based upon such inspection, will be governed by all applicable U. S. and Illinois laws and by University policies.

Computer and Academic Freedom Statement from EFF[488]

The AUP states:

> Personal files on university's computers (for example, files in a user's home directory) should have the same privacy protection as personal files in university-assigned space in an office, lab, or dormitory (for example, files in a graduate student's desk). Private communications via computer should have the same protections as private communications via telephone.

Best Prohibitions Statements

University of Massachusetts at Amherst[489]

The AUP states:

> Clients must only access information that belongs to them, is permitted to them, or is public. Clients must not attempt to decode, crack, or discover passwords that belong to others. UCS may remove clients who are found to possess programs that could be used to access private information that belongs to others.

This part of the AUP is clear and concise. The expectations of the administration have been well stated. However the statements are in terms that a novice computer user may not understand. This AUP also appears to presume guilt

---

[487] University of Illinois at Urbana-Champagne AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

[488] Computer and Academic Statement from the Electronic Frontier Foundation AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

[489] University of Massachusetts at Amherst AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

on the part of the user--the user is guilty until proven innocent (e.g., "[The system administrators] may remove clients who are found to possess programs that could be used to access private information that belongs to others" [490]).

Electronic Frontier Foundation[491]

The AUP states:

> 2. No use of this or any other EFF system as a staging ground to crack other systems...
>
> 4. No use of this or any other EFF system for illegal or criminal purposes...
>
> 9. Obstructing [other people's] work by consuming gratuitously large amounts of system resources (disk space, CPU time) or by deliberately crashing the machine(s) will not be tolerated...
>
> 11. Attempts to read another person's electronic mail or other protected files will be treated with the utmost seriousness"

Best NetNews Statement

University of Wisconsin at Milwaukee[492]

The AUP states:

> That the same standards and principles of intellectual and academic freedom developed for university libraries be applied to material received from the news network. . . That the same standards of intellectual and academic freedom developed for faculty and student publication in traditional media be applied to publication in computer media.

---

[490] University of Massachusetts at Amherst AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

[491] Electronic Frontier Foundation AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

[492] University of Wisconsin at Milwaukee AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Best Due Process Statements

IITF Draft Statement[493]

The AUP states:

B. Redress Principles - Individuals should be protected from harm resulting from inaccurate or improperly used personal information. Therefore, individuals should, as appropriate:

1. Be given means to obtain their information and be provided opportunity to correct inaccurate information that could harm them;

2. Be informed of any final actions taken against them and what information was used as a basis for the decision;

3. Have a means of redress if harmed by an improper use of their personal information.

Computer and Academic Freedom Draft Statement of the EFF[494]

The AUP states:

Suspension or expulsion from a computer is a serious penalty. Users facing these penalties should be given due process protection similar to that given to those facing other serious penalties such as a formal disciplinary warning, a failing grade for cheating, or suspension from class.

Interpretation: Pending action on the charges, the status of a [user] should not be altered, or his [or her] right to be present on the campus and to attend classes [and use computers] suspended, except for reasons relating to his physical or emotional safety and well being, or for reasons relating to the safety and well-being of students, faculty, or university property.

---

[493] Information Infrastructure Task Force's Working Group on Privacy Statement [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

[494] Computer and Academic Freedom Statement of the EFF [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Iowa State University[495]

The AUP states:

Violations of the University Code of Computer Ethics are treated like any other ethical violation as outlined in the Student Handbook and applicable faculty and staff handbooks.

Best Participation in Policy Making and Enforcement Statement

American Association of University Professor's Joint Statement on Rights and Freedoms of Students[496]

The AUP states:

As constituents of the academic community, students should be free, individually and collectively, to express their views on issues of institutional policy and on matters of general interest to the student body. The student body should have clearly defined means to participate in the formulation and application of institutional policy affecting academic and student affairs...the actions of the student government within the areas of its jurisdiction should be reviewed only through orderly prescribed procedures.

The Issues of Privacy, Expression, and Due Process

Policies are often created by computer people not academic-policy experts.[497]

Privacy

One of the most important concepts in an AUP is that of privacy of the users. At most universities, computer files are protected with the same rights as normal property on that campus, and computer accounts are treated as other private space on campuses. "The issue of privacy for computer information is more important than for purely physical goods, as the ease of copying data makes invasions of privacy

---

[495] Iowa State University AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org /11/CAF/policies.

[496] American Association of University Professor's Joint Statement on Rights and Freedom of Students [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

[497] Michael Godwin (personal e-mail July 15, 1996).

synonymous with theft."[498] Many universities regard privacy as a critical component on their computer networks. In the AUP's which have been reviewed, universities endow their systems with privacy in order to provide protection for all their users. These universities have also balanced the concept of privacy with the needs of administering the system.

Universities have recognized that computer files and a user's account space (the $HOME directory) "are a new form of property separable from the media with which they are recorded, and that close analogies can be found between the uses of computer files and of various other forms of physical property."[499] Scholarly thinking and some university policy extends, as nearly as possible, the same protection to computer files as is extended to the analogous physical property.

> Similarly, the computers and computer files of students, staff, and faculty members, being electronic extensions of their personal work areas, may not be inspected, copied, changed, or otherwise tampered with without the permission of the owner, except for purposes relevant to the administration of the computer system.[500]

Most university computer systems have philosophically similar clauses which endow the user's files and e-mail with a large degree of privacy. The privacy statements are *a step in the proper direction*--toward an awareness of the social/community aspects of the Net. However, many universities lack an understanding of the scope and nature of the balance between the user's right to

---

[498] Aidan Low (1995). Right to privacy in the age of telecommunication. Available as of July 1, 1996: http://swissnet.ai.mit.edu/6095/readings-crime.html/low-rule.html.

[499] Aidan Low (1995).

[500] Aidan Low (1995).

privacy and the university's right to violate that privacy. Thus, AUP's have vague policy statements addressing the concept of privacy. The issue is a complicated one, as, clearly, to maintain the system, users' files must sometimes be accessed, but it is unclear when this should happen.

Freedom of Expression

There are those who believe that freedom of speech is a right that is critical in an online world. Yet many universities do not acknowledge that First Amendment rights extend into the electronic world in the same way they do on the real campus and in the real world.

For example, Boston University users must not "transmit or make accessible offensive, annoying or harassing material."[501] "North Dakota State University has a similar policy forbidding *offensive material*."[502] Vague policies like this have traditionally been used by authorities to control speech almost at whim. Anything could be interpreted as "offensive" by someone, and so almost all speech is outlawed by this policy. A number of AUPs have freedom of speech policies which endorse free speech and an open computer system, but, yet, their AUP does not tolerate it.

Accountability is an important issue in regard to freedom of expression on the Internet. While it is reasonable to expect that a message which falls into the category of 'hate mail' be traceable to its author, it is just as reasonable to expect that posting to an Alcoholics Anonymous-type group would not find its way to a user's local

---

[501] Boston University AUP [Online]. Available as of July 1, 1996: gopher://gopher.eff.org /11 /CAF/policies.

[502] Aidan Low (1995).

newspaper or his/her employer. A reality of networked computers is that conversations between and among people in regard to, for example; sex, religion, or a substance abuse discussion group are not nearly as private as they would be if they happened in the real world. On the Net, they are open to a very large number of other people. Conversations within UseNet and on mailing lists are more like a television talk show than they are like semi-private counseling sessions.

As it centers of higher learning, universities should not adopt a policy that restricts free speech nor should they adopt a policy which fosters, for example, the unrestricted sending of *hate mail*.

Due Process

Similar to freedom of speech, due process is a constitutionally protected right "that often does not survive the transition into the world of cyberspace."[503] The difficulty with the proper administration of the concept of due process on the Internet is that the first duty of many system administrators is the continued proper functioning of the network. Endowing the system administrator(s) with responsible for disciplining users who violate the system rules seems to facilitate the *judge, jury, and executioner* model of AUP enforcement. Certainly it is important when the need for disciplinary action arises that the system administrator(s) follow proper procedure. However, given the work load of system administrators and their possible lack of mediation/supervision background, the possibility of due process procedures being followed properly seems to have but a moderate probability of occurring.

---

[503] Aidan Low (1995).

In regard to due process procedures in actual AUPs, there is a seeming lack of even-handedness for infractions.

> The most common penalty for violating rules is the suspension of the account, followed by whatever penalty is judged appropriate. However, the suspension is most often conducted before the investigation of the allegation has even begun. This is clearly a violation of due process, as this gives system administrators the ability to exile people from the system without any sort of review whatsoever.[504]

The Joint Statement on Rights and Freedoms of Students indicates that the most equitable procedure to follow when there is an alleged violation of an AUP is as follows:

> Pending action on the charges, the status of a student should not be altered, or his right to be present on the campus and to attend classes suspended, except for reasons relating to his physical or emotional safety and well being, or for reasons relating to the safety and well-being of students, faculty, or university property.[505]

Suspending students from the university computer system before their guilt has been determined is contrary to the policy just cited when system administrators are given this level of power, they are endowed with "more authority than professors have"[506] to take action for a similar violation occurring, not on the computer network, but in a real classroom.

While many institutions have clearly stated due process procedures for investigations involving alleged AUP violations, many do not. For example, SeasNet (at UCLA) states that an investigation cannot begin without the probability that a given user may be guilty of an offense.

> At Northwestern, the policy makes it clear that user files can be examined and investigations into user accounts begun, but such investigations require the

---

[504] Aidan Low (1995).

[505] Joint Statement on Rights and Freedoms of Students [Online]. Available as of July 1, 1996: gopher://gopher.eff.org/11 /CAF/policies.

[506] Carl Kadie, the managing editor of the Computers and Academic Freedom Archive for the Electronic Frontier Foundation. Kadie, in his review of the University of Hawaii.

> authorization of the Director of the computer system or another clearly defined person. This specification of exactly who can and cannot make these decisions creates an established procedure for the prosecution of offenses against the school.[507]

Due process is an essential right in cyberspace that allows users to know what they can and cannot expect from the systems in which they exist, and is essential for an online society that fosters freedom and openness.

The Future

> Where will rules of use policies be in effect in the future? At present, not all universities provide free speech, privacy protection, and adequate due process for all users, but this will change. As the Internet becomes more and more of a part of everyday life, the overly constrictive policies will be tested again and again, and those without firm support will fall. In time, policies of universities will ensure these three principles of computer rights for citizens of their particular domain of cyberspace.[508]

Explicit Right of Privacy and the Erosion of Privacy Protection

As there is an ever increasing use of technology, an expansion of the legal theory of the intrusion upon privacy is important in order to protect a person's privacy rights in cyberspace. There are legal remedies available when one's privacy rights are violated--when an unwanted person intrudes upon one's seclusion.[509] De May v. Roberts[510] exemplifies the typical case of a physical intrusion where privacy rights may have been violated. In Nader v. General Motors Corporation,[511] the

---

[507] Aidan Low (1995).
[508] Aidan Low (1995).
[509] Arthur R. Miller. (1971). The assault on privacy: Computers, data banks, and dossiers. Ann Arbor, MI: The University of Michigan Press, page 175.
[510] DeMay v. Roberts, 9 N.W. 146 (date), 46 Mich. 160.
[511] Nader v. General Motors, 25 N.Y. 2d 560 (date).

intrusion theory expanded to include non-physical intrusion as well as physical intrusion.[512]

However, Miller observes that due to the "unpromising growth capacity of the common-law theories"[513] there is little immediate prospect for privacy right protection—the technology is advancing far too rapidly for the law to keep pace. As noted in Chapter IV, the right to privacy has evolved quite slowly and often in negative directions since Pavsich v. New England Life Insurance Co.[514]

> Repeatedly, the courts have asked for more legislation in light of the new technology. Unwilling to act as the legislature in a highly technical field, the courts want clearer statutes defining guidelines on the boundaries of privacy of individuals with respect to telecommunication.[515]

Since the right to privacy in common law remains a weak resource for protection, the next alternative seems to call for legislation. Institutions themselves should craft policy to fairly and equitably govern their computer systems. But it seems to be a historical fact of life that "while technology races, legislation crawls,"[516] and, at times, legislation goes in a reverse direction.[517]

Universities need to craft an explicit definition of the scope and nature of privacy for their computer network. This should be done by a broad based committee

---

[512] See also, Katz v. United States, 389 U.S. 347 (1967).

[513] Arthur Miller. (1971). The assault on privacy: Computers, data banks, and dossiers. Ann Arbor, MI: The University of Michigan Press, page 220.

[514] Pavsich v. New England Life Insurance Co., 50 S.E. 68 (1905).

[515] Aidan Low (1995).

[516] Edward V. Long. (1966). The intruders: The invasion of privacy by government and industry. New York: Frederick A. Praeger, page 183. Also see, Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994).

[517] Compare Mutual Film Corp. v. Industrial Comm'n, 236 U.S. 230, 244 (1915) (stating that motion pictures "[are] not to be regarded ...as part of the press of the country") with United States v. Paramount Pictures, Inc., 334 U.S. 131, 166 (1948) (observing that "moving pictures...are included in the press whose freedom is guaranteed by the First Amendment").

consisting of system administrators, policy formulation experts, campus administrators, faculty, staff and students. This wide-based committee should define:

- What a reasonable expectation of privacy consists of, and,
- What portions of the computer network should be totally public.

A Reasonable Expectation of Privacy in Cyberspace

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[518]

In order to apply the Fourth Amendment to computer information which exists in a user's account or in common/public places in cyberspace it is essential to determine the privacy expectations implicit in a search of a user's account or other computer space. In other words, the task at hand is to essentially determine who owns the data/files.

There are three key factors in determining who owns data/files on a computer system. Sergent suggests these factors are "ownership of the computer, ownership of the information involved, and control of or access to the computer and information."[519] The owner of a computer system has the right to possession (Possessory interest) of it. If that computer system is seized for any length of time the owner's Possessory rights will come into play. The owner of the computer system (which would seem to include the stored data) has the right to challenge any searches

---

[518] Katz v. United States, 389 U.S. 347, 361 (1967) (John Harlan, J., concurring).

[519] Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (1995) at 1195.

of the contents due to his/her privacy interest in those contents.[520] This has been substantially clear for computer systems where there has been a one-owner situation. The difficulty arises in determining privacy interests when the computer system has multiple users. The primary issue that arises on multiple-user computer systems is the question as to whether it is possible to have a privacy interest on a computer system that is separate from having ownership or control of the underlying storage media. For examples, in Walter v. United States,[521] United States v. Turk,[522] United States v. David,[523] and Commonwealth v. Parker[524] the Fourth Amendment has been applied to 'searches' involving intangible information. In the cited cases, the searches were treated as searches of the underlying media rather than of the information itself. The Court did not deem these as searches of the data itself. This sidesteps the issue of ownership of the data as a separate issue from ownership of the hardware. Fourth Amendment analysis has typically focused on the search being conducted on a tangible object. The Courts have not addressed the reality that searches of computer spaces can be searches for/of the information that is stored thereon (which is intangible).

As Umar notes, this creates several problems for a search of a multiple user computer system.

> First, one of the goals of modern computer networking is to make the actual physical storage medium or location of information irrelevant to the user of the

---

[520] United States v. Powell, 929 F.2d 1190, 1196 (1991). The owner of truck has standing in court to challenge a search and the of the truck's contents even if the owner was not present at scene.

[521] Walter v. United States, 447 U.S. 649 (1980) (Stevens, J., plurality opinion). In this case, FBI agents were required to obtain a search warrant before viewing films that had been turned over to them by a third party.

[522] United States v. Turk, 526 F.2d 654, 666 (1976), cert. denied, 429 U.S. 823 (1976). This case involved the legal seizure of a cassette tape, but playing tape without a warrant was ruled an impermissible search.

[523] United States v. David, 756 F.Supp. 1385, 1392-93 (1991) Law enforcement officials legally seized an electronic databook, but warrant was required to access its contents.

[524] Commonwealth v. Parker, 619 A.2d 735, 742 (1993) The Court ruled that a search warrant was required to listen to a cassette tape which was legally seized.

> system. A legal focus upon the physical media may create difficult line drawing problems, because a logically unitary group of information may be strewn across multiple computer systems and different types of storage media.
>
> Second, the development of software protection for user privacy does not affect physical control of the computer system's storage media; the computer's owner or manager can access anything stored on the system. By the same token, the user has no control over where or how her data is physically stored. If control of the physical media is the important criteria, the owner might be able to object to a search of a computer, but no one else could.[525]

In this situation, Sergent notes, there would be conflict when applying a metaphor where a telephone search was the target.

> A telephone user does not control the transmission facilities. The telephone company has as much of an opportunity to record conversations as the system manager of a multiple-user computer system has to investigate user files. Lack of control of the underlying media, however, has not [deprived] the telephone user of an expectation of privacy in the contents of her conversation. Although a computer user has no control over where data is physically stored, his data is conceptually stored in a unitary area under his control. By focusing on characteristics of this conceptual data area, courts can create rules to apply to a broad spectrum of physically divergent computer systems.[526]

Privacy Interests on a University Computer System

It would appear that users of a university's on-line computer network should have some expectation of privacy. In order for a user to have a reasonable expectation of privacy, "two conditions need to exist: 1) the data or file(s) must not have knowingly been exposed or given to another person, and, 2) the system manager's ability to access that data/file(s) cannot constitute an illegal disclosure if the contents of the data/file(s) were given/disclosed to another person."[527]

Information placed in areas which are generally accessible by other users of a multi-user system appear to lose all protection of privacy as so many other people will have access to that data. Just as there can be no expectation of privacy in a cordless telephone conversation (where the broadcast can be intercepted and listened to by

---

[525] Amjad Umar. (1993). Distributed computing. Englewood Cliffs, NJ: Prentice Hall, page 201.

[526] Sergent at 1196-1197.

[527] Sergent at 1197-1198.

anyone), there can be no expectation of privacy on a multi-user computer system when data is stored in an area that is accessible to other average system users.[528]

Existing laws are relevant to the issues inherent in crafting a university's AUP, but they are, at times, ambiguous and seemingly in conflict with each other. The mere fact that an intrusion, under certain circumstances, could be a legal invasion of privacy does not automatically obviate the existence of a reasonable expectation of privacy. The Supreme Court has required more than just legal protection exist in order to generate an expectation of privacy.[529]

In a university setting, given the number of users that have legitimate access rights, it is advisable to deploy a stated social convention in regard to acceptable use of the system. The university can determine how much or how little privacy is appropriate/suited to their needs. What is important is the strength and pervasivness of the convention. This strength of statement is important, as it will determine the reasonableness of expecting users to adhere to it. If the convention is inherently weak, the courts will view the policy statements as not much more than suggestions (which are generally unenforceable).[530] If a convention is drafted which defines privacy and establishes the degree to which it exists, in order to be legally effective

---

[528] United States v. Smith, 978 F.2d 171, 179 (1992). The Court stated that, "Courts should bear in mind that the issue is not whether it is conceivable that someone could eavesdrop on a conversation but whether it is reasonable to expect privacy.", cert. denied, 113 S. Ct. 1620 (1993); State v. Howard, 679 P.2d 197, 206 (1984). The Court found no reasonable expectation of privacy for owners of cordless phones where owner's manual explained the nature of the phone, and therefore allowing police to monitor and record conversations.

[529] Oliver v. United States, 466 U.S. 170, 177-78 (1984). The Court held that even though law enforcement officers committed trespass to search defendant's property, there was no Fourth Amendment violation because defendant could have no reasonable expectation of privacy in an open field; California v. Greenwood, 486 U.S. 35, 43 (1988) (quoting Oliver, 466 U.S. at 178. The Greenwood court declared that the "Fourth Amendment analysis must turn on ... our societal understanding that certain areas deserve the most scrupulous protection from government invasion."

[530] California v. Greenwood at 40 nn.2-4 (1988). This case involved a the belief, on the part of but a few, that a general convention exists which prohibits snooping in other people's garbage (which is at the curbside awaiting pickup by the refuse collection company). The Court took great pains to minimize any convention-based argument by emphasizing the variety of ways any such convention could be violated.

that convention should be generally (widely) known to the users of the computer system. As demonstrated in Greenwood and Oliver, the Supreme Court relies on underlying social norms/expectations[531] in order to determine if a law is to stand or be struck down.

Sergent notes that the courts will not want to endow law enforcement agencies with the responsibility to determine the explicit and implicit privacy relationships among the users of a computer system, and between the users and the system administrator(s) therefore, the convention (law, policy, etc.) should be firmly and clearly stated, and should be widely available to those who are impacted.[532]

Lacking stated policy (or convention) establishing the notion that privacy does in fact exists on a computer system, one should assume no expectation of privacy, even given the presence of leveled access and passwords. Sergent notes that "[i]t also can be argued that because computer networks are so new, there has not been time for any privacy conventions to evolve."[533]

Thus the social convention appears to be that lacking any stated policy in regard to privacy expectations on a computer system, one should assume that privacy does not exist.

Even with the advent of software which allows computer users to have 'mailboxes' and computer spaces that exclude other users from casually reading their

---

[531] California v. Greenwood at 44. The Court held that the existence of a state law conferring a right of privacy unto a person's garbage (at curbside awaiting disposal) was irrelevant and the right did not exist. The Court called the laws "no less than a *suggestion* that concepts of privacy under the laws of each State are to determine the reach of the Fourth Amendment [emphasis added]."

[532] Sergent at 1199; Oliver, 466 U.S. at 181 (quoting New York v. Belton, 453 U.S. 454, 458 (1981) (quoting Wayne LaFave, Case-By-Case Adjudication versus Standardized Procedures: The Robinson Dilemma, 1974 S.Ct. Rev. 127, 141)). The Oliver court, in rejecting a case by case approach to the Fourth Amendment, said it refused to impose '[a] highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions.'

[533] Sergent at 1199 n.98.

mail or rummaging about in their files, this does not confer the user with a reasonable expectation of privacy.[534]

On the other hand, it could be argued that a computer system user does have a reasonably expectation of privacy as today's software has firewalls and security such that in order to access the mailbox and account space of another, a person should attack and defeat those firewalls and security measures. Technology may not have reached to point where one can legally expect privacy on a computer system, but we are quickly approaching that time. Where cordless telephone communications still lack the protection of the Fourth Amendment, the Court in United States v. Smith noted that:

> Although we express no opinion as to what features or circumstances would be necessary to give rise to a reasonable expectation of privacy, it should be obvious that as technological advances make cordless communications more private at some point such communication will be entitled to Fourth Amendment protection.[535]

Thus far, the focus has been upon what reasonable expectation of privacy exists in regard to other system users, and upon disclosures of data/files. The system manager, however, has the unique ability to access any and all areas of the system at will. It is Sergent's belief that the "system manager's ability to access user data does not constitute disclosure, because the manager is in a distinctive position not shared by other users of the computer system."[536] Sergent also notes that it may be reasonable to believe that the mere fact that a third party (in this case the system

---

[534] Oliver v. United States, 466 U.S. 170, 182 (1984). The court's reasoning was that: "It is true, of course, that ... Oliver ... planted the marihuana upon secluded land and erected fences and "No Trespassing" signs around the property. And it may be that because of such precautions, few members of the public stumbled upon the marihuana crops seized by the police. Neither of these suppositions demonstrates ... that the expectation of privacy was legitimate in the sense required by the Fourth Amendment; See also, Note, From Private Places to Personal Privacy: A Post-Katz Study of Fourth Amendment Protection, 43 N.Y.U. L. Rev. 968, 983 (1968). The expectation of privacy must be justified as well as reasonable in order to qualify for Fourth Amendment protection.

[535] United States v. Smith, 978 F.2d 171, 180 (1992).

[536] Sergent at 1200.

manager) is privy to information may relieve the user of any Fourth Amendment reasonable expectation of privacy protection. There are a number of instances where the disclosure of information to another person or organization (similar to a computer system manager) has been found not to substantiate a claim (by a user) that a reasonable expectation of privacy existed.[537] For example, courts have found that persons in situations similar to a system administrator have disclosed information that was given to them and have not been held liable for those disclosures. Smith v. Maryland[538] was involved with the disclosure of telephone numbers, United States v. Miller[539] with bank deposit records, United States v. Willis[540] with motel records, United States v. Choate[541] with addresses on the outside on envelopes, People v. Perlos[542] with medical records, and State v. Smith[543] with social service records. From this, one may reasonably conclude that an individual has no expectation of privacy when any information is kept/maintained by any third party (with the exception of lawyer-client like situations).

In contrast, it may be argued that the system operator is a neutral being, and that the data contained on the computer system was never disclosed to (or intentionally shared with) the system operator. Thus there is a reasonable expectation of privacy on the part of the user in regard to the role of the system manager's ability to read/view/disclose data.

Sergent divides data into two categories:

> The first type includes information used to operate the computer system. By analogy to the disclosure cases, there is no legitimate expectation of privacy in these records.

---

[537] Sergent at 1200.
[538] Smith v. Maryland, 442 U.S. 735, 741-42 (1979).
[539] United States v. Miller, 425 U.S. 435, 442 (1976).
[540] United States v. Willis, 759 F.2d 1486, 1498 (1985), cert. denied, 474 U.S. 849 (1985).
[541] United States v. Choate, 576 F.2d 165, 175 (1978), cert. denied, 439 U.S. 953 (1978).
[542] People v. Perlos, 462 N.W.2d 310, 321 (1990).
[543] State v. Smith, 367 N.W.2d 497 (1985).

> The second type of users information consists of personal information the system manager has no need to access. The user can have a reasonable expectation of privacy in this information because "the operator is not an intended recipient of the information, nor is he expected to use the information for his own purposes." Some information that a user may wish to keep private does not fit neatly into these categories. Courts have room to increase or decrease significantly the scope of privacy protection depending on how they draw the boundaries of these categories.[544]

It would appear that there are areas and situations where a computer user has a reasonable expectation of privacy and that right should be respected. It also appears that there are many more areas on a computer system where a user may believe that privacy exists, but such is not the case. Whatever position is taken it is of primary importance that the university widely disseminate its policy.

Cyberspace as a Totally Public Place

Cyberspace could be viewed as though it is composed of 99% public terrain and 1% private property, and policy could be established with that in mind. To accomplish this, for the purposes of search and seizure, searches of cyberspace should be viewed as metaphorically akin to an airport baggage search or to a search of an occupied motel room. A university's computer system should not, under any circumstances except for standing statutes, be viewed as the user's private property.

A university's computer systems should be viewed as one views an airport. An airport and a border crossing point are critical zones in which special Fourth Amendment considerations apply. At an airport, security officials are allowed broad latitude in regard to what, who, and how they may search.[545] Computer systems, like airports, are uniquely subject to terrorist attacks if extraordinary methods are not allowed.

---

[544] Sergent at 1202.

[545] United States v. Moreno, 475 F.2d 44 (1973), cert. den. 414 U.S. 840 (1973), 94 S.Ct. 94.

Although airport statistics show that only six percent of the passengers frisked were found to have weapons, such probability nevertheless justifies the frisk in view of the substantial interest in preserving the integrity and safety of air travel.[546] Given even this small percentage of 'weapons possessions' and even smaller likelihood of those weapons being used against passengers, the Supreme Court has ruled that airport officials are justified in conducting searches and seizures beyond the constraints normally imposed upon such actions.[547]

For the purposes of search and seizure, a university's computer system might also be viewed as a hotel or motel where registration as a guest constitutes *implied consent*[548] to motel and hotel employees to enter occupied rooms in the performance of their duties.

This chapter has presented the major issues and provided insight into these issues. The next chapter will summarize these findings and offer some suggestions for developing and managing Acceptable Use Policy documents.

---

[546] United States v. Bell, 335 F.Supp. 797 (1971), aff'd 464 F.2d 667 (1971), cert. den. 409 U.S. 991 (1972), 93 S.Ct. 335 (An anti-hijacking system at an airport has been held to be constitutional).

[547] Krauss v. Superior Court of San Joaquin County, __ __ __ (date), 96 Cal.Rptr. 455, 478 P.2d 1023 (ovrld on other grounds by People v. Cook, 22 Cal.3d 67 (date), 148 Cal.Rptr. 605, 538 P.2d 130).

[548] Massachusetts Fair Information Practices Act, M.G.L. Chapter 66A, §§1-3.

CHAPTER V

CONCLUSIONS AND RECOMMENDATIONS

Introduction

This chapter will present the author's conclusions, recommendations and opinions based upon the foregoing research, and, will provide support for those conclusions, recommendations and opinions by citing other authors and publications.

An Overview

Originally, the Internet was

> . . . a smattering of university and military computers linked together in a nationwide *network of networks*. Policies at most of these nodes in this continental web were generally fairly open, as the only people who had access to these systems were a small group of people who knew each other well. Passwords were rare, and privacy was not an issue at many of these places . . . Users trusted each other to act responsibly when using the system, and altercations between users were rare. However, there were extreme sanctions on use of the system, particularly on what could or could not be performed on the computer systems. The machines were extremely expensive, and even a small program could take days to run, so it was difficult to convince those in charge of the machine of the need to run a program."[549]

In the intervening years there have been significant changes in the Internet. Most noticeable have been the changes in the recent two to four year period. The universities that comprised the original Internet have grown, and now practically every college is connected to the Internet. Along with the expansion of the Internet, and of the use of computers in general, has come a dramatic growth in the number of

---

[549] Aidan Low (1995). Right to privacy in the age of telecommunication. Available as of July 1, 1996: http://swissnet.ai.mit.edu/6095/readings-crime.html/low-rule.html.

people who use this global network. However, the rules, customs, and metaphors governing the use of university computer systems have not changed, either in nature or substance. But, they should change in response to the changed nature of the network user.[550]

The society which inhabits the Internet and local area networks, like any emerging society, needs its own set of rules and customs. However, cyberspace does not have one set of rules, but, thousands. These 'rules' vary from "near-anarchistic code[s] of complete freedom to authoritarian [codes which deny] … all rights."[551] AUP's generally lack content that would cause them to be more of a social contract. The AUP should set a philosophical guidepost for the community of users in the way the U.S. Constitution sets philosophical guideposts—in the way the student and faculty handbooks provide guideposts for the campus community.

The social contract by which we live in our real world community is the U.S. Constitution. While many members of the U.S. community may not be able to identify Constitutional principles, they are well aware of them. Members of the U.S. community understand concepts of the Constitution, and tend to live by them. These Constitutional concepts are not meant primarily as rules for law enforcement officials but as foundational principles upon which our entire U.S. community is based. So, too, should an AUP be a philosophical guidepost for the community of users on the Internet and on university computer networks. The Internet and the university computer network have become social instruments. The university AUP should reflect

---

[550] Bruce Sterling. (1995). The hacker crackdown. New York: Bantam Books, page 247.
[551] Aidan Low (1995). Right to privacy in the age of telecommunication.

that paradigm shift. To accomplish this, AUP's should address social issues (e.g., privacy, freedom of speech, access, overuse of the resources), not merely the pragmatic and operational issues (e.g., change your password frequently, do not share your password with anyone, do not run wasteful computation-intensive programs) of computer networks.

Universal Similarities of Computer Use Policy

The policy statements which have been identified in Chapter IV as being in the 'best' category appear (philosophically) in many other university AUP statements. These statements are worthy of emulation as they appear to:

1. consider the human condition and/or the capabilities of computer system,
2. conform to federal statutes and/or campus policy,
3. state their intent in a clear and unambiguous way, and,
4. account (when appropriate) for the social nature of the network.

Commercial activity not related to the instutition's mission was banned on almost every system surveyed and reviewed in this dissertation. However, the statements which forbade 'commercial use' of the network were generally over-broad. For example, the University of Miami's AUP forbids commercial use of their network, but School of Law students are required to serve an internship (often in the commercial sector) which requires the students to, *de facto*, use the network for

commercial purposes. The university administrators and the law school administrators are in the process of revising the 'no commercial use' statement.[552]

In a number of cases, institutions have statements that appear to be based upon a lack of understanding of the appropriate uses of certain computer applications (software). For example, many institutions prohibit needless waste of their system's resources by logging into MUDs, playing games, or running wasteful computation-intensive programs. For an education major, using, exploring, and running MUD software may be a legitimate use of system resources, while, if a finance major were doing this, it might not be a legitimate use of system resources.

Some aspects of policy statements make sense, should be used widely, and should be accepted as they are. These statements, for the most part, are ones that deal with operational and mechanical issues of the computer and the network.

Many other aspects of policy statements also make sense, but the universities tend to state them in a vague and overly broad manner. These statements tend to deal with the social and community aspects of the computer networks. This is an area of great concern as this appears to be the area where the greatest conflict will occur (e.g., harassment complaints, invasions of privacy, fair use of resources). This may be attributed to the situation that many institution's computer policy committees are still, usually, composed exclusively of computer operations experts.

Another common theme among university AUP's is the formulation of policy statements fashioned in ignorance of: a. the actual workings of computer systems, and, b. the human condition. For example:

---

[552] Dr. Michael Froomkin (personal e-mail, June 12, 1996).

> [A]n old policy at Rice University forbade "running file commands on large filesystems." Under this ruling, a student looking at her partition of a large fileserver would be in violation of this rule. At the University of South Florida, the rules forbid running a computer program on the network which "interferes" or "affects the performance of" any other computer on the network. Rules phrased in this way are meaningless, as every computer program running on a network takes a little bit of bandwidth away from every other computer program, and so this rule outlaws all computer use on the network. Here, technical mistakes about the nature of the network are being made, because the authors of the policy do not understand the nature of the system that they are regulating.[553]

Also, for example, the University of Massachusetts Computer Security and Usage Standards draft document states that authorized users must:

> not store their access passwords in batch files, in automatic login scripts, in terminal function keys, in computers without access control, or in other locations where another person might discover them[554]

The human condition appears to be such that this AUP statement will be ignored by the users as, it: 1. creates a situation where users are informed that it is against policy to write their passwords down *anywhere*, and, 2. ignores the fact that virtually all terminal software allows for automatic login scripts and terminal key macro creation.

Another difficulty occurs when the computer policy of a school conflicts with the policy that governs the real campus. For example, Northwestern University's AUP advises the victims of harassment to speak to their Information Systems' representatives. However, the school policy on sexual harassment makes it quite clear that, in such cases, complaints should be directed to the dean. Policy statements should be consistent with the rules and regulations within the campus community at

---

[553] Aidan Low (1995). Right to privacy in the age of telecommunication.

[554] Information Technology Subcommittee. (1996, July). Computer security and usage standards [In-press]. Boston, MA: University of Massachusetts Board of Trustees, page 3.

large. It would also be a wise first step to explore the possibility that computer use policy is identical to real life statutes and campus policy whenever possible.

Ownership of the Computer System and the Computer Network

A common misconception among university administrators is that, since the physical network and the actual computers and fileservers belong to them, all the data stored on them belongs to them as well.

> This is an extremely dangerous policy, largely because of its implications on intellectual property. If a student writes a paper on a school computer, does the school then own the paper? If that student then compiles a computer program on that computer, does it then belong to the university?[555]

There are a few universities that have policies based on the '*We own the physical equipment, therefore, we own everything stored on it'* philosophy. For example, Boston University "reserves the rights to: limit or restrict any account holder's usage, inspect, copy, remove or otherwise alter any data, file, or system resource."[556] This policy allows the institutional personnel to do anything they desire with a user's account and the information in that account.[557] Such policies are clearly contrary to the standards found on real life campuses.

> A far more logical policy is to regard the computer accounts of a university as the dorm rooms of students or office space of faculty, belonging to the university but yet the private space of the individuals who live there.[558]

---

[555] Aidan Low (1995). Right to privacy in the age of telecommunication.

[556] Boston University AUP [Online]. Available as of July 1, 1996: gopher://gopher.eff.org /11/CAF/policies.

[557] Dr. Carl Kadie (personal e-mail, May 20, 1996).

[558] Aidan Low (1995). Right to privacy in the age of telecommunication.

Recommendations for Crafting an AUP

The following items are taken from the text of this dissertation. They are noted here as they are important principles given the philosophy of dissertation. These points will, hopefully, serve as the basis for an institution's senior administrator 'charge' to an AUP committee as they embark on the task of creating policy.

1. From page 56. Thus, it seems appropriate that the university can define what a computer user's expectations of privacy are through its Acceptable Use Policy (AUP).

From page 79. There are a number of elements which must be present in order for an invasion of privacy to be actionable. The information accessed must otherwise be private, secluded, or secret,[559] there must be lack of consent by the owner of the facts,[560] and/or the intrusion must involve public disclosure[561] of facts which are otherwise private. *Some* authorities have also held that a physical intrusion or something analogous to a trespass *must* occur.[562]

From page 81. There are a number of flavors of privacy, and a University community should come to a consensus on which flavor it desires.

From page 82. When crafting an AUP, a foundation issue will be the determination of the scope and limits of privacy on a given computer system. A clarification of privacy as a global principle for computers, as a principle for individual systems, as a non-existent principle, or as some combination of these needs to be established before other concerns are addressed. Deciding this will facilitate the

---

[559] Dortch v. Atlanta Journal, 405 S.E.2d 43 (1991), 261 Ga. 350.

[560] Leggett v. First Interstate Bank of Oregon, 739 P.2d 1083 (1987), 86 Or.App. 523.

[561] Dortch v. Atlanta Journal, 405 S.E.2d 43 (1991), 261 Ga. 350; Steele v. Offshore Shipbuilding, 867 F.2d 1311 (1989), reh den 874 F.2d 821 (1989) and McCullough v. Offshore Shipbuilding, 874 F.2d 821 (1989).

[562] Garner v. Triangle Publications, 97 F.Supp. 546 (1951), Hogin v. Cottingham, 533 So.2d 525 (1988), McDaniel v. Coca-Cola Bottling, 2 S.E.2d 810 (1939), 60 Ga.App. 92.

process of developing a basis of thought upon which other issues (e.g., computer as a newspaper, office desk, common carrier, broadcaster, etc.) will rely. Establishing the basic notions of *public* and *private* in regard to on-line computer systems is critical in order to build a foundation upon which resolution of other issues will be based.

2. From page 83. Lacking legal clarity on a number of issues, a University needs to establish policy—its AUP—in order to clarify the 'ground rules' for the entire community of users. Furthermore, as a chief source of litigation is failure to properly prepare for legal eventualities, having an AUP in place will greatly aid in reducing potential exposure to litigation.

3. From page 86. The University administration has been established to protect everyone's rights and to insure that everyone's rights and responsibilities are properly addressed and protected. The stakeholders in the creation of policy should be constantly reasserting, in their minds, that crafting policy is a positive activity and should benefit and protect all.

4. From page 107. There should be a balance between a user's expected right to privacy and the administration's right to insure the continued operation of its systems. This balancing should be crafted into an AUP in order for it to be effective.

5. From page 104. For the purposes of crafting a university AUP, the notion should be established throughout the AUP that 'personal property rights' as we know them in the real world do not necessarily apply to a university computer system.

6. From page 112. It is important, on the part of a university, to establish its position that a computer account is *not* a private secluded place. Establishing *private places* would create a situation where users have a reasonable expectation that their *space* will not be invaded. If the situation is such that the computer users have an

expectation of privacy in their accounts, then any rummaging about or intermeddling with privacy is searching within the meaning of the Fourth Amendment.[563]

A university should establish the belief (policy) that computer accounts and disk space are not immune from observation by appropriate university employees conducting tasks related to the rendition of service to the computer system and its users.

7. From page 112. So, too, will the 'privacy' area of the AUP play against the 'freedom from unreasonable search and seizure' area of the AUP. These antithetical positions force balance, and this tension will provide a sounding board to assure that the 'privacy' principles and statements in the AUP are valid and reasonable. It is an advantage when developing an AUP to craft the Search and Seizure statements in concert with the 'privacy' area as the First and Fourth Amendments are built and measured on mutual ground.[564]

---

[563] State of Maine v. Barclay, 398 A.2d 794, 796 (1979); State v. Richards, 269 A.2d 129, 134 (date).

[564] Harvey A. Silverglate and Thomas C. Viles. (1991, May). Constitutional, legal, and ethical considerations for dealing with electronic files in the age of cyberspace. Paper presented at the 1991 Federal Enforcement Conference, Georgetown University Law Center, Washington, DC. The courts recognize that the First and Fourth Amendments grew from the same historical source, for the struggle for press freedom was energized by the struggle against the license to print, and against the prior restraints imposed by the Crown to enforce the license. In the Supreme Court's words, "the struggle for the freedom of the press was primarily directed against the power of the licensor ... And the liberty of the press became initially a right to publish 'without a license what formerly could be published only with one.'" While this freedom from previous restraint upon publication cannot be regarded as exhausting the guaranty of liberty, the prevention of that restraint was a leading purpose in the adoption of that constitutional provision. Lovell v. City of Griffin, Ga., 303 U.S. 444, 452 (1938). The Supreme Court commands that special care be taken when authorizing or reviewing a search involving any entity engaged in the publication or dissemination of ideas. "Freedom of the press" long has been interpreted broadly to protect not only newspapers publishers and pamphleteers, e.g., Lovell, Id., 303 U.S. at 452, but also motion pictures, Roaden v. Kentucky, 413 U.S. 496 (1973); Burstyn v. Wilson, 343 U.S. 495, 502 (1952); United States v. Paramount Pictures, 334 U.S. 131, 166 (1948), and even computer bulletin boards, Legi-Tech v. Keiper, 766 F.2d 728, 734-35 (1985), from prior restraints and general searches. In order to avoid prior restraints on speech, the particularity requirement of the Fourth Amendment "is to be accorded the most scrupulous exactitude when the 'things [to be seized]' are books, and the basis for their seizure is the ideas which they contain." Stanford v. State of Texas, 379 U.S. 476 (1965) reh den, 380 U.S. 926 (1965), citing Marcus v. Search Warrant of Property, 367 U.S. 717 (1961).

8. From page 126. The university should deal with the concept of 'information privacy' in its AUPs 'due process' statement, or should clearly specify a 'due process' philosophy in its AUP.

9. From page 131. The AUP should now be a social contract in addition to being the 'owners manual.'

10. From page 158. Universities need to craft an explicit definition of the scope and nature of privacy for their computer network. This should be done by a broad based committee consisting of system administrators, policy formulation experts, campus administrators, faculty, staff and students. This wide-based committee should define:

- What a reasonable expectation of privacy consists of, and,
- What portions of the computer network should be totally public.

Important Thoughts and Considerations

The following items are taken from the text of this dissertation. They are noted here as they are important thoughts and considerations given the philosophy of dissertation.

- From page 110. This rationale of 'knowing exposure' is problematic in that it has been extended such that even disclosure of a bit of information causes one to completely loose Fourth Amendment protection of the information in question. It should not be that a person's privacy protection rights under the Fourth Amendment are totally lost merely due to law enforcement's ability to procure (otherwise protected) information from a third party (by any means).

- From page 112. So, too, will the 'privacy' area of the AUP play against the 'freedom from unreasonable search and seizure' area of the AUP. These antithetical positions force balance, and this tension will provide a sounding board to assure that the 'privacy' principles and statements in the AUP are valid and reasonable. It is an advantage when developing an AUP to craft the Search and Seizure statements in concert with the 'privacy' area as the First and Fourth Amendments are built and measured on mutual ground.[565]
- From page 158. In order to apply the Fourth Amendment to computer information which exists in a user's account or in common/public places in cyberspace it is essential to determine the privacy expectations implicit in a search of a user's account or other computer space. In other words, the task at hand is to essentially determine who owns the data/files.
- From page 162. Lacking stated policy (or convention) establishing the notion that privacy does in fact exists on a computer system, one should assume no expectation of privacy, even given the presence of leveled access and passwords. Sergent notes that "[i]t also can be argued that because computer networks are so new, there has not been time for any privacy conventions to evolve."[566]
- From page 165. A university's computer systems should be viewed as one views an airport. An airport and a border crossing point are critical zones in which special Fourth Amendment considerations apply. At an airport, security officials are allowed broad latitude in regard to what, who, and how they may search.[567] Computer systems, like airports, are uniquely subject to terrorist attacks if extraordinary methods are not allowed.

---

[565] Harvey A. Silverglate and Thomas C. Viles. (1991, May). Constitutional, legal, and ethical considerations for dealing with electronic files in the age of cyberspace.

[566] Sergent at 1199 n.98.

[567] United States v. Moreno, 475 F.2d 44 (1973), cert. den. 414 U.S. 840 (1973), 94 S.Ct. 94.

- From page 166. For the purposes of search and seizure, a university's computer system might also be viewed as a hotel or motel where registration as a guest constitutes *implied consent*[568] to motel and hotel employees to enter occupied rooms in the performance of their duties.
- From page 179. The Net is a growing and evolving community, and this dissertation suggests that the paradigm for AUP creation/revision should change to reflect the views the Net as a shared community resource.
- From page 182. Drawing models of privacy and search and seizure with the intent of applying them to Acceptable Use Policies may not be realistically possible.[569] Easterbrook[570] and de Sola Pool[571] suggest that looking to our legal system for guidance is not yet possible. The legal community is still in the process of analyzing the phenomenon known as cyberspace. They are in the process of setting doctrine which will legally define actions in cyberspace. Even with clear legal foundational guidance from the legislature and the courts, there may be specific concerns that will not be addressed by courts examining privacy and other Constitutional questions, but which will apply to the development of Acceptable Use Policies.

---

[568] Massachusetts Fair Information Practices Act, M.G.L. Chapter 66A, §§1-3.

[569] David R. Johnson and Kevin A. Marks, Mapping Electronic Data Communications Onto Existing Legal Metaphors: Should We Let Our Conscience (And Our Contracts) Be Our Guide?, 38 Villanova L. Rev. 487, 488 (1993).

[570] Frank H. Easterbrook. (1995, November). Cyberspace and the law of the horse. Paper presented at the University of Chicago Legal Forum's Symposium on the Law of Cyberspace, Chicago, Illinois. Available as of July 1, 1996: http://www-law.lib.uchicago.edu /forum /easterbrook.doc.

[571] Ithiel de Sola Pool. (1983). Technologies of freedom. Cambridge, MA: Belknap Press. page 7.

Transformation of the Paradigm for Crafting Acceptable Use Policy

Existing Acceptable Use Policy (AUP) primarily regulates user-to-computer behavior. But there has been a radical change and a demographic shift in both the nature of the clientele and the physical capability of the Internet. The Net is fast becoming a mirror of a real world community, rather than an information resource or an information superhighway. Those who craft policy should adjust their paradigm for formulating policy—a paradigm which currently seems to be based upon the construct of the network as a mechanical entity. The Net is a growing and evolving community, and this dissertation suggests that the paradigm for AUP creation/revision should change to reflect the views the Net as a shared community resource. In order to reformulate the paradigm to one which addresses social and communal needs, those who craft AUP's should have a foundational understanding of the legal concepts of privacy, search and seizure, and due process. They should also have a working understanding of the principles and theories of managing and setting policy for commonly shared resources (figure 4).

Overview

An on-line computer system is too often viewed as an area where students and employees have few, if any, rights and responsibilities. Many University AUPs declare that the students and employees are liable to be summarily removed (from the computer system) without due process for trivial violations of the rules. An AUP should instill and, to a large degree, explain the philosophy that *a person who violates*

the University rules while using the on-line computer system will be treated in the same manner as a person who violates the rules on the physical campus.

> The Fourteenth Amendment requires due process before a governmental entity, such as a public institution, may deprive one of life, liberty, or property. In a college setting, a student's good name and reputation are considered a 'liberty' right, and a student's right to attend college is considered a 'property' right. Due process would be required before a student is deprived of either at a public institution.
>
> Substantive processes require, essentially, that policies and rules must be related to the basic government purpose at hand that basic fairness be employed. For instance, college rules should be related to educational matters and applied fairly. Procedural due process generally refers to the requirement of notice and hearing before being deprived of a right. For example, before being expelled for misconduct, students should have notice of what they have done wrong and a chance to tell their side of the story.[572]

And it continues to note that: "[T]he degree of specificity required [in codes of conduct] is that which would allow a student to adequately prepare a defense against the charge. [The University] should make plain the prohibited conduct, the procedure for determining whether a student is engaged in such conduct, and what the penalty is."[573]

Privacy

> Technological change often outpaces the law. Examining the legal implications of emerging technologies can help narrow this gap. Although the precise contours of the new media technologies are not yet known, certain radical evolutions in the way we receive, transmit, and utilize information have already become apparent.[574]

---

[572] Patricia A. Hollander, D. Parker Young, and Donald D. Gehring. (1985). A practical guide to legal issues affecting college teachers. Boulder, CO: Westview Press.

[573] Patricia A. Hollander ., D. Parker Young, and Donald D. Gehring. (1985).

[574] Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994). See generally, Anne M. Fulton, Cyberspace and the Internet: Who Will Be The Privacy Police?, 3 Comm. Law Conspectus 63 (1995).

The possibilities engendered by the Information Superhighway will evolve in many ways. "Two evolutions—infinite choices and interactivity—will have profound

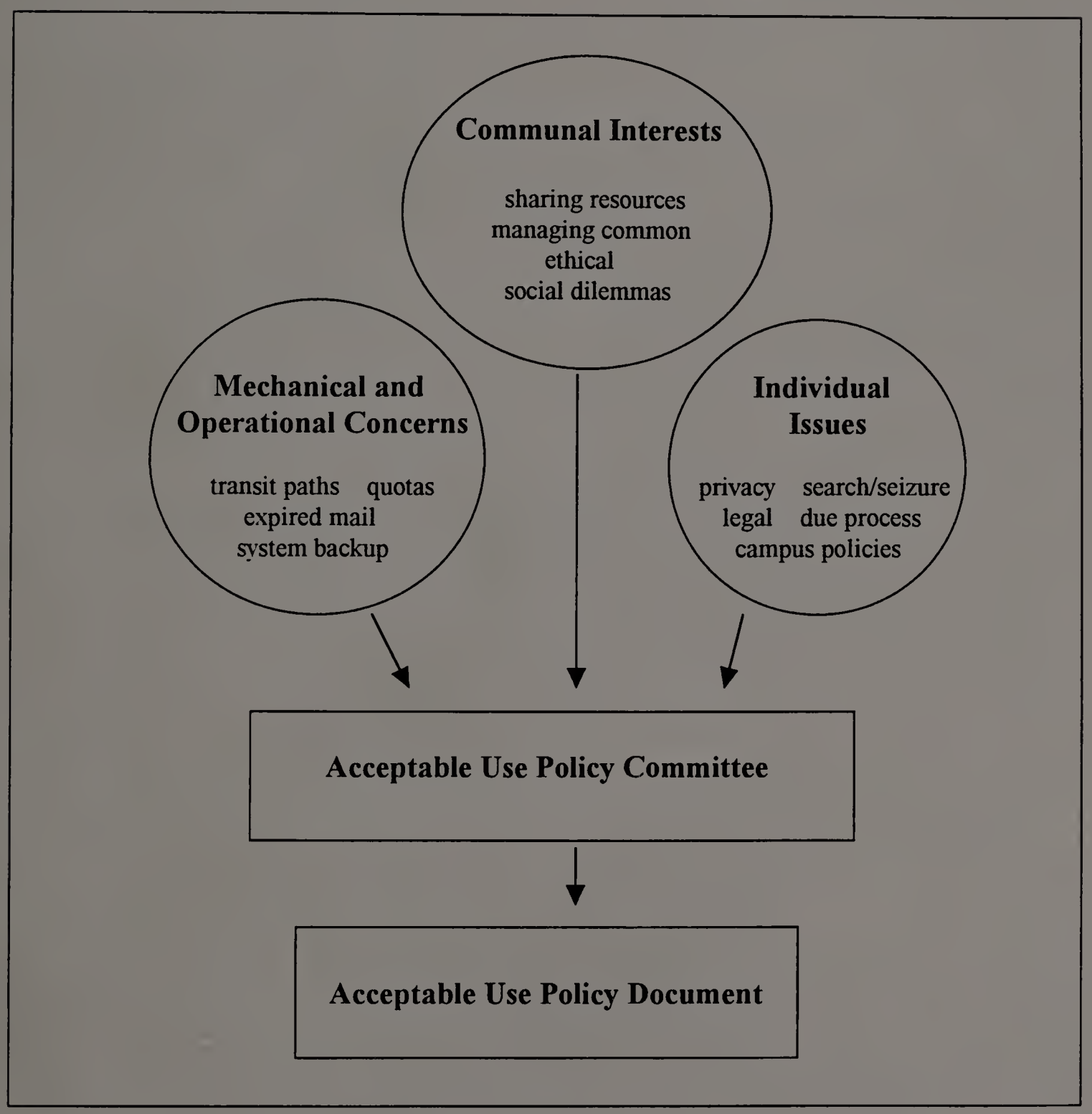

Figure 4 - Model for AUP Creation

impact"[575] on, *inter alia*, the need to revisit Constitutional issues in order to reassess their application to user policy issues. This reality is beginning to impact federal legislators. This is a positive event and we can look forward to a coherent national policy regarding the nature of cyberspace. But until that time, those who must create institutional Acceptable Use Policy should develop their own understanding of what constitutes fair and equitable policy in this environment which has warped our sense of the law.

> Privacy is a major issue of our day.
>
> > There seems to be no legal issue today that cuts so wide a swath through conflicts confronting American society [as Privacy]. From AIDS tests to wiretaps, polygraph tests to computerized data bases, the common denominator has been whether the right to privacy outweighs other concerns of society ...[576]

A Louis Harris poll (figure 3) supports the position that Privacy, the root of a number of present issues, is a significant concern of the American people.

Drawing models of privacy and search and seizure with the intent of applying them to Acceptable Use Policies may not be realistically possible.[577] Easterbrook[578] and de Sola Pool[579] suggest that looking to our legal system for guidance is not yet

---

[575] Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1062 (March 1994).

[576] Robert Ellis Smith. Quoted in Andre Bacard. (1995). The computer privacy handbook. Berkeley, CA: Peachpit Press. page 17.

[577] David R. Johnson and Kevin A. Marks, Mapping Electronic Data Communications Onto Existing Legal Metaphors: Should We Let Our Conscience (And Our Contracts) Be Our Guide?, 38 Villanova L. Rev. 487, 488 (1993).

[578] Frank H. Easterbrook. (1995, November). Cyberspace and the law of the horse. Paper presented at the University of Chicago Legal Forum's Symposium on the Law of Cyberspace, Chicago, Illinois. Available as of July 1, 1996: http://www-law.lib.uchicago.edu /forum /easterbrook.doc.

[579] Ithiel de Sola Pool. (1983). Technologies of freedom. Cambridge, MA: Belknap Press, page 7.

possible. The legal community is still in the process of analyzing the phenomenon known as cyberspace. They are in the process of setting doctrine which will legally define actions in cyberspace. Even with clear legal foundational guidance from the legislature and the courts, there may be specific concerns that will not be addressed by courts examining privacy and other Constitutional questions, but which will apply to the development of Acceptable Use Policies.

There is a need for universities to craft local rules for a computer network. There may also be compelling reasons for universities to craft their own AUP, because the AUP may, even for public institutions, "boil down to a matter of contract,"[580] as they are in private institutions. Thus universities should research the issue of privacy as it applies to on-line computer systems. Even if an Acceptable Use Policy is eventually deemed to be a contract, there still remains a need to base the AUP upon the same concepts which are inherent in the U.S. Constitution.

Search and Seizure

The Computer—technology's latest tool in communications—has forced us to re-engineer our policy in regard to the balance between individual privacy and society's need for information. This new communications technology has ushered in a new era of global access where even the least powerful in society have a significant voice. However, the technology has generated the possibility that corporations and

---

[580] Daniel Burk (personal e-mail, April 6, 1996).

the government will be the beneficiaries of Orwellian powers. The outcome of this will be determined by the underlying societal values, and not by the technology itself. Sergent notes that this is an "apparent … clash between data privacy [concerns] and law enforcement's need to gather evidence in criminal investigations."[581]

In recent years, it has become apparent that we have an ever diminishing degree (and amount) of control over what personal information of ours is available - and available to just about anyone.[582] Neither the law enforcement establishment nor society in general seems to have kept fully abreast of the changing technological times. As a result, our privacy has been severely eroded. Unless a better understanding is achieved in regard to the relationship of cyberspace to our real world paradigms, we may soon find that 'privacy' is non-existent.

Sergent advocates for a "framework by which the Fourth Amendment can be applied to a range of activities involved in computer investigation without hampering the legitimate needs of law enforcement."[583] To develop these frameworks, Sergent suggests that the Supreme Court should extend its current analysis:

> [O]f the scope and content of the Fourth Amendment to [include] searches and seizures of computer information. Because the level of privacy we enjoy in personal information depends upon value choices made by our society, examining legal norms is an important part of the process of making those choices. As new technology evolves, the Supreme Court's Fourth Amendment methodology is likely

---

[581] Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (1995).

[582] Larry Tye. (1993, September 5). Privacy lost in high-tech era. Boston Sunday Globe, page 18-19. This article detailed the extent to which supposedly private information was actually publicly available in this day in age.

[583] Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (1995).

> to favor security over privacy. The model [put in place should involve] more emphasis to privacy.[584]

Kapor and Godwin[585] warn of computer searches and seizures based upon the American Bar Association's (ABA) Criminal Justice Section suggested search and seizure guidelines. Kapor and Godwin are concerned that the ABA's position amazingly seems to be based upon three publications[586] from the Department of Justice's National Institute of Justice. Kapor and Godwin note that:

> 1. There was no guidance to the magistrate as to when the computer or related equipment should not be seized, either because it is not necessary as evidence or because such a seizure would intolerably *chill* the lawful exercise of First Amendment rights or abridge a property owner's Fourth Amendment rights.
>
> 2. There was inadequate recognition of the business or individual computer owner's interest in continuing with lawful commercial business, which might be hindered or halted by the seizure of an expensive computer.
>
> 3. There was no effort to measure the likelihood that investigators would find computers equipped with such justice-obstructing measures as automatic erasure software or *degausser* booby-trapped hardware, the presence of which might justify a no-knock search and seizure, among other responses.[587]

---

[584] Randolph S. Sergent, Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81 Va. L. Rev. 1181 (1995).

[585] Mitchell Kapor, and Michael Godwin. (1994). Civil liberties implications of computer searches and seizures: Some proposed guidelines for magistrates who issue search warrants [On-line]. Available as of July 1, 1996: http://www.eff.org/pub/Publications/Mike_Godwin /search_and_seizure_guidelines.eff.

[586] J. McEwan. (1989). Dedicated computer crime units. Washington, DC: National Institute of Justice.; D. Parker. (1989). Computer crime: Criminal justice resource manual. Washington, DC: National Institute of Justice; C. Conly. (1989). Organizing for computer crime investigation and prosecution. Washington, DC: National Institute of Justice.

[587] Mitchell Kapor, and Michael Godwin. (1994). Civil liberties implications of computer searches and seizures: Some proposed guidelines for magistrates who issue search warrants [On-line].

Tragedy of the Unmanaged Common

"Since the barrier between the natural and computer sciences is often high and opaque, it is best to first discuss the *tragedy of the commons*"[588] as Hardin[589] outlined the concept. This will be followed by a discussion of the possible implications of the *tragedy* for online computer systems.

> In 1968, biologist Garrett Hardin brought to science's attention a little-known work by the nineteenth century amateur mathematician William Forster Lloyd on population growth and control. Lloyd examined the fate of a *common* pasture shared among rational, utility-maximizing herdsmen.[590]

Shepherds grazed sheep on the individual parcels of land they owned. But there was another pasture, a large public stretch of land held in reserve, owned in *common* by the villagers and known, logically enough, as the *Common*. Then, some shepherds became greedy. They began guiding their sheep to the *Common* each day, preferring to wear out the public pasture because they thought it cost them nothing and saved their own small patches. Soon, others joined in, unwilling to deplete their lands while a few neighbors took advantage of the public lands. It wasn't long before the *Common* was turned into a muddy wasteland—useless to anyone. And as the shepherds watched their individual pastures fall to overgrazing, they realized that their village had been sacked by its own people. They'd stolen their shared livelihood, economic

---

[588] Roy M. Turner. (1991, January). The tragedy of the commons and distributed AI systems [Online]. Paper presented at the 12th International Workshop on Distributed Artificial Intelligence, University of New Hampshire, Durham, NH. Available as of July 1, 1996: http://cdps.umcs.maine.edu /Papers /1993/TofCommons/TR.html.

[589] Garret Hardin. (1968). The tragedy of the commons. Science, (162), page 1243-1248.

[590] Roy M. Turner. (1991, January). The tragedy of the commons and distributed AI systems [Online].

security, cultural center, and much of their village's beauty from themselves and their children.[591]

Once a resource is being utilized at a rate near its carrying capacity, additional utilization will degrade its value to its current users. Users then will enter into a cycle of additional use of the resource to gain or to try to break even, as others use it. Since all users engage in this behavior, the resource is ultimately and inevitably doomed.

For example, the Ogallala Aquifer, once known as the largest body of fresh water on earth, stretches under West Texas and as far north as Nebraska. Each year, farmers pump out five trillion gallons of water more than the rains put back into the aquifer. Recent conservation measures and heavy rains have helped reverse the fall in groundwater levels, but the Ogallala Aquifer is still so low that the next generation may find the costs to pump it are prohibitive. The depletion of the largest of nine major aquifers underlying the state is just one of the serious environmental challenges facing West Texas and many other mid-Western states.[592]

> Ruin is the destination toward which all men rush, each pursuing his own best interest in a society that believes in the freedom of the common.[593]

The inexorable working out of the resource's ruin is Hardin's tragedy of the common. In human affairs, the tragedy of the common has never been more evident than it is today. Its effects are pollution, global warming, ozone depletion, overfishing and extinction of species, abuse of aquifers, and destruction of the rain forests.

---

[591] Garret Hardin. (1968). The tragedy of the commons. Science, (162), page 1243-1248.
[592] __. (1991). Where breakdown and bankruptcy play. The Economist, page 21.
[593] Garret Hardin. (1968). The tragedy of the commons. Science, (162), page 1243-1248.

But what relevance does this have for Acceptable Use Policy?

Relating this to the creation of Acceptable Use Policy creation is relatively easy as, at the heart of these models/research projects, is the problem of the free-rider or the overgrazer, and the issue of regulating use of a shared resource.

As Ostrom notes, the challenge becomes how a group can "organize and govern themselves to obtain collective benefits in situations where the temptations to free-ride and/or to break commitments are substantial."[594] Ostrom[595] studied a "wide range of communities which had a long history of successfully producing and maintaining collective goods. She also studied a number of communities which had failed partially or completely in meeting this challenge."[596] In comparing the communities, Ostrom found that groups which are able to organize and govern themselves are marked by the following design principles:

- Group boundaries are clearly defined
- Rules governing the use of collective goods are well matched to local needs and conditions
- Most individuals affected by these rules can participate in modifying the rules
- The rights of community members to devise their own rules is respected by external authorities
- A system for monitoring member's behavior exists; this monitoring is undertaken by the community members themselves
- A graduated system of sanctions is used
- Community members have access to low-cost conflict resolution mechanisms[597]

---

[594] Elinor Ostrom. (1990). Governing the commons: The evolution of institutions for collective action, page 27.

[595] Elinor Ostrom. (1990). Governing the commons: The evolution of institutions for collective action, page 30.

[596] Peter Kollock and Marc Smith. (1994). Managing virtual communities: Cooperation and conflict in computer communities [On-line]. Available as of November 1, 1996: http://www.sscnet.ucla.edu/soc/csoc/vcommons.htm.

[597] Peter Kollock and Marc Smith. (1994). Managing virtual communities: Cooperation and conflict in computer communities [On-line].

Applying Ostrom's observations along with a foundational understanding of the legal principles of privacy, search and seizure, and due process seems to provide a powerful model upon which the crafting of a public higher education's AUP can be based (see Figure 4 - page 181).

The AUP as a Social Contract - A Transformational Approach

> The social contract reflects the agreement between the people and the government on how much power the people consent for the government to have and exert. The social contract between the people and the government exists so long as the government uses its powers within the due process of law and the people agree to the outcome of the due process of law. With the due process of law as a vehicle for maintaining the social contract, the government uses its power without compromising certain *natural and inalienable* rights of the individuals in a way unspecified by the Constitution, our social contract. Hence, by allowing the government to expand its power at the expense of the right to privacy breaches the contract between the people and the government because such action compromises the individual rights without the consent from the people.[598]

Currently, an Acceptable Use Policy tends to be a *Ten Commandment*-like document which, at various levels of friendliness, informs the users what is expected of them in regard to user-to-computer actions and, in a vague and overly broad manner, what is expected in regard to user-to-user behavior. These *Ten Commandment*-like AUP's were *apropos*, however, with the changing demographics of the typical university, and the increasing social use capability of the Net, the computer user policy (the AUP) should also change. The AUP should become more of a social contract. The AUP should be crafted, as other social contracts are (e.g., the US Constitution, a faculty handbook, a student handbook). Those who craft the AUP should certainly consider the logistical needs inherent in maintaining a secure

---

[598] Right to privacy in the age of telecommunication [On-line]. (1996, March 26).

and functional computer network. In addition, those who craft the AUP should also come to the realization the computer network is much more than a place where hackers and pornographers roam freely,[599] or where the primary focus is the survivability and functionality of the system. They should view the network as a community of people who congregate to seek and/or exchange information, knowledge, and, wisdom.

> For many people, the Internet has been like a worldwide, multimillion member think-tank, available 24 hours a day to answer any question, from the trivial to the scholarly. This magical knowledge-multiplying quality comes from the ongoing cooperative effort of many thousands of people, who freely contribute their expertise in response to questions. That precious power of a large group of people to act as a collective thinktank for each other is vulnerable to human folly. A relatively small number of malefactors hold the power to mess up a good thing for a far larger number of cooperative citizens.[600]

The Acceptable Use Policy can be a way to manage the electronic *common* that will preserve the power of cooperation without infringing on individual freedom or the growth of knowledge and wisdom of which the Net is capable. "The collective intelligence of the Net ought to get a chance to activate a social immune response before too many people who don't know exactly what they are panicking about call for a police force we don't need."[601]

There is a more-or-less subtle, but none the less, transformational change that those who craft a university's AUP should undergo. Those who craft AUP's should shift their paradigm from one which views a computer usage policy (the AUP) as a document that informs the user primarily of what the technical and logistical

---

[599] Howard Reingold. (1996, June 15). Federal judges defend free speech on the Internet [Online]. Posted to the Virtual Communities Conference on the WELL (Whole Earth Lectronic Link), San Francisco, CA.

[600] Howard Reingold. (1996). The tragedy of the electronic commons [Online].

[601] Howard Reingold. (1996). The tragedy of the electronic commons [Online].

requirements of computer network usage are to one which includes the view that an AUP—a computer usage policy—is also a social contract:

1. that is crafted by a demographically representative committee of campus community members,

2. that will facilitate the development of community, which will, in turn, facilitate the establishment of community-endorsed ethics and values.

To accomplish this, it is necessary that those who comprise an AUP development committee be familiar with the issues that have been put forth in this study (see figure 4 - page 181). Familiarity with the issues of privacy and search and seizure will provide a scholarly understanding of how the legal system views such issues in the real world. This understanding will hopefully assist those who craft AUP's in:

- creating statements that treat computer network actions in the same manner that they would be treated if they occurred in the real world, and,
- providing a foundational basis for addressing social issues/dilemmas which may develop.

This study also supports the concept of a basic paradigm shift in AUP's toward becoming social contracts. This author believes that the first step toward creating AUPs that are social contracts is an understanding of basic social/community issues which all appear to flow from the right to privacy.

This dissertation concludes that regulations need to be in place to govern the acceptable use of computer networks. These AUP's should be locally developed by those who have a foundational understanding of:

- legal principles of privacy, search and seizure, and due process, and,
- theory of management of commonly shared resources and the inherent questions of social order.

BIBLIOGRAPHY

Author's Note: A number of citations contained in this study refer to legal material. The legal citations vary somewhat, in form, from the traditional APA references. Legal materials are cited in conformance with the APA Publication Manual's (p. 223) requirement to utilize the conventions in the Bluebook: A Uniform System of Citation (1991).

General References

Adam, John A. (1992, August). Cryptography=privacy? IEEE Spectrum, 29(8).

Allgeyer v. Louisiana, 165 U.S. 578 (1897).

American Association of University Professor's Joint Statement on Rights and Freedom of Students [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

American Psychological Association. (1994). Publication manual of the American Psychological Association (4th ed.). Washington, DC: Author.

Amsterdam, Anthony G., Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 384 (1974).

State of Arizona v. Childs, 519 P.2d 854 (1974).

Arizona v. Hicks, 480 U.S. 321 (1987).

Armstrong v. Manzo, 380 U.S. 545 (1965).

AUP-Working Group of Internet Engineering Task Force. (1995, July). Acceptable use policy definition [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

Ball, Milner S. (1985). Lying down together: Law, metaphor and theology. Madison, WI: University of Wisconsin Press.

Baer, Walter S. (1993, January-February). Technology's challenges to the First Amendment. Telecommunications Policy, 17(1).

Bailey v. Richardson, 341 U.S. 918 (1951).

Banisar, David. (1993, July). Battle for control of encryption technology. IEEE Software, 10(4).

Barber v. Time, Inc., 159 S.W.2d 291 (1942).

Barlow, John Perry. (1990). Crime and puzzlement [On-line]. Available as of July 1, 1996: http://www.eff.org/pub/Publications John_Perry_Barlow /crime_and_puzzlement.1.

Barlow, John Perry. (1993, November). A plain text on crypto policy. Communications of the ACM, 36(11).

Barry v. City of New York, 712 F.2d 1554 (1983).

Bayse, William A. (1993, March). To tap or not to tap. Communications of the ACM, 36(3).

Beall, Robert, Note, Developing a Coherent Approach to the Regulation of Computer Bulletin Boards, 7 Computer L. J. 499 (1987).

Beard v. Akzona, 517 F.Supp.128 (1981).

Beck, Henry, Control of, and Access to, On-Line Computer Data Bases: Some First Amendment Issues in Videotex and Teletext, 5 Hastings Comm/Ent L. J. 1 (1982).

Becker, Loftus E. Jr., The Liability of Computer Bulletin Boards for Defamation Posted by Others, 22 Conn. L. Rev. 203 (1989).

Becker, Lynn, Electronic Publishing: First Amendment Issues in the Twenty-First Century, 13 Fordham Urb. L. J. 801 (1985).

Bequai, August. Technocrimes. (1987). Lexington, MA: D.C. Heath and Company.

Berkshire Cablevision, Inc. v. Burke, 571 F.Supp. 976 (1983), vacated, 773 F.2d 382 (1985).

Berlin, Isaiah. Two concepts of liberty. In Four essays on liberty. (1969). London: Oxford University Press.

Bier, William C. (1980). Privacy: A vanishing value? New York: Fordham University Press.

Bills v. Aseltine, 958 F.2d 697 (1992).

The bluebook: A uniform system of citation (15th ed.). (1991). Cambridge, MA: Harvard Law Review Association.

Board of Regents v. Roth, 408 U.S. 564 (1972).

Boston University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Brandenberg v. Ohio, 395 U.S. 444 (1969).

Branscomb, Lewis M., and Anne M. Branscomb. (1993, March). To tap or not to tap. Communications of the ACM, 36(3).

Branscum, Deborah. (1991, March). Ethics, e-mail, and the law. MacWorld, 8(3).

Brinegar v. United States, 338 U.S. 160 (1949).

Brody, Herb. (1992, November-December). Of bytes and rights. Technology Review, 95(8).

Burstyn v. Wilson, 343 U.S. 495 (1952).

Caden, Marc L. and Stephanie E. Lucas, Comment, Accidents on the Information Superhighway: On-Line Liability and Regulation [On-line], 2 Rich. J.L. & Tech. 3 (1996). Available as of July 1, 1996: http://www.urich.edu/~jolt /v2i1/caden_lucas.html.

Calder v. Bull, 3 U.S. 386 (1798).

California Penal Code, §502.

California v. Acevedo, 500 U.S. 565 (1991).

California v. Ciraolo, 476 U.S. 207 (1986).

California v. Greenwood, 486 U.S. 35 (1988).

Cangialosi, Charles, The Electronic Underground: Computer Piracy and Electronic Bulletin Boards, 15 Rutgers Computer & Tech. L. J. 265 (1989).

Canon, Maggie. (1994, June). Yank the clipper. MacUser, 10(6).

Cantrell v. Forest City Pub., 419 U.S. 245 (1974).

Carey v. Population Serv. Int'l, 431 U.S. 678 (1977).

Cason v. Baskin, 20 So.2d 243 (1945).

CAUSE Current Issues Committee. (1995, Summer). Current issues for higher education information resources management. Cause/Effect.

Cavazos, Edward A., Note, Computer Bulletin Board Systems and the Right of Reply: Redefining Defamation Liability for a New Technology, 12 Rev. Litig. 231 (1992).

Cefalu v. Globe Newspaper, 391 N.E.2d 935 (1979), 8 Mass. App. 71, 5 Media L.R. 1940, cert den and app dismd 444 U.S. 1060 (1979), 62 L.Ed.2d 738, 100 S.Ct. 994, reh den 445 US 973 (1980), 64 L.Ed.2d 251, 100 S.Ct. 1669.

Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557 (1980).

Chambers v. Maroney, 399 U.S. 42 (1970).

Charles, Robert, Note, Computer Bulletin Boards and Defamation: Who Should Be Liable? Under What Standards?, 2 J.L. & Tech. 121 (1987).

Chlapowski, Francis S., Note: The Constitutional Protection of Information Privacy, 71 B.U. L. Rev. 133 (1991).

Cohen, Morris, and Robert Berring. (1989). How to find the law. St. Paul, MN: West Publishing.

Cohen v. California, 403 U.S. 15 (1971).

Colorado v. Bertine, 479 U.S. 367 (1987).

Columbia Human Rights Law Review. (1973). Surveillance, dataveillance, and personal freedoms: Use and abuse of information technology. Fair Lawn, NY: R.E. Burdick.

Commonwealth v. Parker, 619 A.2d 735 (1993).

Communications Decency Act of 1995, 47 U.S.C. 151.

Computer and Academic Statement from the Electronic Frontier Foundation AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11 /CAF/policies.

Conly, C. (1989). Organizing for computer crime investigation and prosecution. Washington, DC: National Institute of Justice.

Covington v. Houston Post, 743 S.W.2d 345 (1988).

Creech, Kenneth C. (1993). Electronic media law and regulation. Boston: Focal Press.

Cubby v. Compuserve, 766 F.Supp 135 (1991).

Cummings v. Walsh Constr. 561 F.Supp 872 (1983).

Cutrera, Terri A., Computer Networks, Libel and the First Amendment, 11 Computer L. J. 555 (1992).

Cutrera, Terri A., Note, The Constitution in Cyberspace: The Fundamental Rights of Computer Use, 60 U.M.K.C. L. Rev. 139 (1991).

Dalhousie University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Declaration and Resolves of the First Continental Congress, Journals of Congress I (1800).

Denning, Dorothy E. (1993, March). Wiretapping and cryptography. IEEE Spectrum, 30(3).

Denning, Dorothy E. (1993, July-August). The clipper encryption system. American Scientist, 81(4).

Denning, Dorothy E. (1993, March). To tap or not to tap. Communications of the ACM, 36(3).

Denning, Dorothy E. (1993, March). Final thoughts. Communications of the ACM, 36(3).

De Young, R. and S. Kaplan. (1988). On averting the tragedy of the commons. Environmental Management, 12, page 283-293.

Dibbell, Gibbs. (1990, July 24). On line and out of bounds, Village Voice.

Di Cato, Edward M., Operator Liability Associated with Maintaining a Computer Bulletin Board, 4 Software L. J. 147 (1990).

Dierks, Michael H., Computer Network Abuse, 6 Harv. J.L. & Tech. 307 (1993).

Di Lello, Edward V., Functional Equivalency and Its Application to Freedom of Speech on Computer Bulletin Boards, 26 Colum. J.L. & Soc. Prob. 199 (1993).

Dortch v. Atlanta Journal, 405 S.E.2d 43 (1991), 261 Ga. 350.

Dred Scott v. Sanford, 60 U.S. 393 (1857).

Dunne, Robert L., Deterring Unauthorized Access to Computers: Controlling Behavior in Cyberspace Through a Contract Law Paradigm, 35 Jurimetrics J. 1 (1994).

Dutton, William H. (1992, July). The social impact of emerging telephone services. Telecommunication Policy.

Dyson, Freeman. (1979). Disturbing the universe. New York: Harper and Row.

Easterbrook, Frank H. (1995, November). Cyberspace and the law of the horse. Paper presented at the University of Chicago Legal Forum's Symposium on the Law of Cyberspace, Chicago, Illinois. Available as of July 1, 1996: http://wwwlaw.lib.uchicago.edu/forum /easterbrook.doc and /~easterbrook.fn.

Eisenstadt v. Baird, 405 U.S. 438 (1972).

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508 (1986).

Electronic Freedom Foundation AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

Elmer-DeWitt, Philip. (1993, January 18). Who's reading your screen? Time.

Elmer-Dewitt, Philip. (1994, March 14). Who should keep the keys. Time.

Elmore v. Atlantic Zayre, 341 S.E.2d 905 (1986).

Factors Ect. v. Pro Arts, 579 F.2d 215 (1978).

Faucher, John D., Comment, Let the Chips Fall Where They May: Choice of Law in Computer Bulletin Board Defamation Cases, 26 U.C. Davis L. Rev. 1045 (1993).

Fed. R. Evid. 101(3).

Fishman, B., and R.D. Pea. (1994). The internetworked school: A policy for the future. Technos: Quarterly of Education and Technology, 3(1).

Flaherty, David H. (1972). Privacy in colonial New England. Charlottesville: Univ. of Virginia Press.

Fogel v. Forbes, 500 F.Supp. 1081 (1980), 6 Media L. Rev. 1941.

Fourth Annual Benton National Moot Court Competition: System Operator Liability for Defamatory Statements Appearing on an Electronic Bulletin Board, 19 J. Marshall L. Rev. 1107 (1986).

Fox, Dennis R. (1985). "Psychology, Ideology, Utopia, and the Commons." American Psychologist 40(1), page 48-58.

Freedman, Warren. (1987). The right of privacy in the computer age. New York: Quorum Books.

Freeh, Louis. (1993, December 8). Hampering new telecom technology to make it easily wiretappable. Presented at the National Press Club, Washington, D.C.

Fried, Charles, Constitutional Doctrine, 107 Harv. L. Rev. 1140 (1994).

Garner v. Triangle Publications, 97 F.Supp. 546 (1951).

Garramone Gina M., Uses of Political Computer Bulletin Boards, 30 J. of Broadcasting and Electronic Media 325 (1986).

Gates, William F. (Interviewee). (1996, March 25). The CBS evening news. New York: Columbia Broadcasting System, Inc.

Gerety, John. Redefining Privacy, 12 Harv. C.R.-C.L. L. Rev. 233 (1977).

Gibran, Kahlil. (1923). The prophet. New York: Phoenix Press.

Gibson, William. (1984). Neuromancer. New York: Ace Books.

Gifis, Steven. (1991). Law dictionary. New York: Barron's.

Gilbert, Jonathan. Note, Computer Bulletin Board Operator Liability for User Misuse, 54 Fordham L.Rev. 439 (1985).

Gillard v. Schmidt, 579 F.2d 828 (1978).

Goals 2000: Educate America Act, Pub. L. No. 103-227 (1994).

Godwin, Michael. (1995, June 16). Constitutional problems with the Communications Decency Amendment: A legislative analysis by the Electronic Frontier Foundation. EFFector 8(10) [On-ine]. Available as of July 1, 1996: http://www.eff.org/pub/EFF/Newsletters /EFFector/#8.

Godwin, Michael. (1993, March). To tap or not to tap. Communications of the ACM 36(3).

Godwin, Michael. (1995, March). No copycat criminal: LaMacchia case reveals a federal attitude problem. Internet World. Available as of July 1, 1996: http://swissnet.ai.mit.edu /6095/readings-crime.html#Required

Goldberg v. Kelley, 397 U.S. 254 (1970).

Goodrich v. Waterbury Republican-American, 448 A.2d 1317 (1982).

Gore, Albert. (1990, July 15). Networking the future: We need a national "superhighway" for computer information. Washington Post, page B3.

Goss v. Lopez, 419 U.S. 565 (1975).

Graves, William, Carol Jenkins and Anne Parker. (1995, Summer). Development of an information policy framework. Cause/Effect.

Griswold v. Connecticut, 381 U.S. 479 (1965).

Hardin, Garrett. (1968). The tragedy of the commons. Science (162), page 1243-1248.

Hardin, Garrett. (1977). Managing the commons. San Francisco: W.H. Freedman and Co.

Hardy, Trotter, The Proper Legal Regime for Cyberspace, 55 U. Pitt. L. Rev. 993 (1994).

Harms v. Miami Daily News, 127 So.2d 715 (1961).

Hartman v. Meredith Corp., 638 F.Supp. 1015 (1986).

Hester v. United States, 265 U.S. 57 (1924).

Hixson, Richard F. (1987). Privacy in a public society: Human rights in conflict. New York: Oxford University Press.

Hoffman, Lance J. (1973). Security and privacy in computer systems. Los Angeles: Melville Publishing Company.

Hogin v. Cottingham, 533 So.2d 525 (1988).

Hollander, Patricia A., D. Parker Young, and Donald D. Gehring. (1985). A practical guide to legal issues affecting college teachers. Boulder, CO: Westview Press.

Holmes, Oliver Wendell Jr., The Path of the Law, 10 Harv. L. Rev. 457 (1897).

Illinois v. Lafayette, 462 U.S. 640 (1983).

Industrial Foundation of the South v. Texas Industrial Accident Board, 540 S.W.2d 668 (1976).

Information Infrastructure Task Force's Working Group on Privacy Statement [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Institute for Transfer of Technology to Education (ITTE). (1995). Plans and policies for technology in education. Alexandria, VA: National School Boards Association.

State of Iowa v. Raymond, 142 N.W.2d 444 (1966).

Iowa State University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Jahnke. (1990, November 14). The cops come to cyberspace. Boston Magazine.

James Madison University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Jensen, Eric C., Comment, An Electronic Soapbox: Computer Bulletin Boards and the First Amendment, 39 Fed. Comm. L. J. 217 (1987).

Johnson, David R. and Kevin A. Marks., Mapping Electronic Data Communications Onto Existing Legal Metaphors: Should We Let Our Conscience (And Our Contracts) Be Our Guide?, 38 Villanova L. Rev. 487 (1993).

Johnson, Nancy P., Robert C. Berring, and Thomas A. Woxland (1993). Winning research skills (2nd ed.). St. Paul, MN: West Publishing.

Johnson, T. L. (1990, April 10). Fred the computer: Electronic newspaper services seen as 'ad-ons'. Comm. Daily, 4.

Johnson v. United States, 333 U.S. 10 (1948).

Joint Anti-Fascist Refugee Comm. v. McGrath, Anti-Soviet Friendship v. McGrath, International Workers Order v. McGrath, 341 U.S. 123 (1951).

Joint Statement on Rights and Freedoms of Students [Online]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

Junker, John M., The Structure of the Fourth Amendment: The Scope of the Protection, 79 Crim. L. & Criminology 1105 (1989).

Justice Society (Committee on Privacy). (1983). Privacy and the law. London: Fontana Paperbacks.

Kahn, John R. (1989). Defamation liability of computerized bulletin board operators and problems of proof. Available as of July 1, 1996: http://www.eff.org /finish.

State of Kansas v. Howard, 679 P.2d 197 (1984).

Kansas State University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Kapor, Mitchell and Michael Godwin. (1994). Civil liberties implications of computer searches and seizures: Some proposed guidelines for magistrates who issue search warrants [On-line]. Available as of July 1, 1996: http://www.eff.org /pub/Publications/Mike_Godwin/search_and_seizure_guidelines.eff.

Kapor, Mitcheli. (1996). Where is the digital highway really heading? Available as of November 1, 1996: http://www.hotwired.com/wired/1.3/features /kapor.on.nii.html.

Katsh, M. Ethan., The First Amendment and Technological Change: The New Media Have a Message, 57 Geo. Wash. L. Rev. 1459 (1989).

Katsh, M. Ethan., Law in a Digital World, 38 Villanova L. Rev. 403 (1993).

Katz v. United States, 389 U.S. 347 (1967).

Kleiner, Kurt. (1993, September 18). Cracking into the world of whispers. New Scientist, 139, 14-15.

Kollock, Peter, and Marc Smith. (1994). Managing virtual communities: Cooperation and conflict in computer communities [On-line]. Available as of November 1, 1996: http://www.sscnet.ucla.edu/soc/csoc/vcommons.htm.

Konefsky, Samuel J. (1974). The legacy of Holmes and Brandeis: A study in the influence of ideas. New York: DeCapo Press.

Kratka, Josh. (1990). For their eyes only: The insurance industry and consumer privacy. Boston: Massachusetts Public Interest Research Group.

Krauss v. Superior Court of San Joaquin County, ___ ___ ___ (date), (ovrld on other grounds by People v. Cook, ___ ___ ___ (date)).

Kwong Hai Chew v. Colding, 344 U.S. 590 (1953).

LaFave, Wayne R., Case-By-Case Adjudication versus Standardized Procedures: The Robinson Dilemma, 1974 S.Ct. Rev. 127.

LaFave, Wayne R. (1987/1994). Search and seizure: A treatise on the Fourth Amendment (2nd ed.). St. Paul, MN: West Publishing.

Lakoff, George and Mark Johnson. (1980). Metaphors we live by. Chicago: University of Chicago Press.

Lan, Nguyen. (1995, Aug. 13). Virginia man's computer seized in Internet lawsuit. Washington Post, page B6.

LeClair v. Hart, 800 F.2d 692 (1986).

Ledsinger v. Burgmeister, 318 N.W.2d 558 (1982).

Leggett v. First Interstate Bank of Oregon, 739 P.2d 1083 (1987).

Legi-Tech v. Keiper, 766 F.2d 728 (1985).

Levin, Carol. (1993, November 23). Digital privacy: Who has the right to read your data? PC Magazine,12(20), page 29.

Lincoln Fed. Labor Union v. Northwestern Iron & Metal Co., 335 U.S. 525 (1949).

Lindsey v. State, 204 N.E.2d 357 (1965).

Linowes, David F. (1989). Privacy in America: Is your private life in the public eyes? Chicago: University of Illinois Press.

Lippmann, Walter. (1914). A preface to politics. New York: M. Kenerley Publishing.

Lochner v. New York, 198 U.S. 45 (1905).

Long, Edward V. (1966). The intruders: The invasion of privacy by government and industry. New York: Frederick A. Praeger.

Los Angeles v. Preferred Communications, Inc., 476 U.S. 488 (1986).

Looney, Donna Mohr. (1992). The essentials of legal citation. St. Paul, MN: West Publishing.

Loundy, David J., E-Law: Legal Issues Affecting Computer Information Systems and System Operator Liability, 3 Alb. L. J. Sci. & Tech. 79 (1993).

Loundy, David J. (1990). E-Law 2.0: Computer information systems law and system operator liability revisited. Available as of July 1, 1996: http:// www.leepfrog.com/E-Law/E-Law/Contents.html.

Lovell v. City of Griffin, Ga., 303 U.S. 444 (1938).

Low, Adian. (1995). Right to privacy in the age of telecommunication. Available as of July 1, 1996: http://swissnet.ai.mit.edu/6095 /readings-crime.html/low-rule.html.

Luker, Mark. (Interviewee). (1996, August 17). The future of the Internet. Washington journal [Television]. Atlanta, GA: Turner Network News, Inc.

Lynn v. Allied Corp., 536 N.E.2d 25 (1987).

MacNeil, Heather. (1992). Without consent: The ethics of disclosing personal information in public archives. Metuchen, NJ: The Scarecrow Press, Inc.

Magenis v. Fisher Broadcasting, 798 P.2d 1106 (1990).

Maggs, Peter B., John T. Soma and James A. Sprowl. (1992). Computer Law, Cases, Comments, Questions. St. Paul, MN: West Publishing, page 490.

State of Maine v. Barclay, 398 A.2d 794 (1979).

Malloy, Rich. (1991, October 15). Technology is not the problem. Byte, 16(11).

Mankato State University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Marcus v. Search Warrant of Property, 367 U.S. 717 (1961).

Markoff, John. (1990, May 13). Some computer conversation is changing human contact. NY Times, page 1.

Marron v. United States, 275 U.S. 192 (1927).

Marx, Gary T. (1993, March). To tap or not to tap. Communications of the ACM, 36(3), page 41.

Massachusetts Commission on Computer Technology and Law. (1993, February 1). Computer crime laws: A report to the governor. Boston, MA: Author.

Massachusetts Fair Information Practices Act, Massachusetts General Laws, Chapter 66A, §§1-3.

Mavity v. Tyndall, 66 N.E.2d 755 (1946), 224 Ind. 364, appeal after remand 74 N.E.2d 914 (1948), 225 Ind. 360, appeal dismissed Indiana on relation of Mavity v. Tyndall, 68 S.Ct. 609 (1948), 333 U.S. 834, 92 L.Ed. 1118, reh den 68 S.Ct. 732 (1948), 333 U.S. 858, 92 L.Ed 1138.

McCall v. Courier-Journal and Louisville Times, 623 S.W.2d 882 (1981), cert den 456 U.S. 975 (1982).

McCullough v. Offshore Shipbuilding, 874 F.2d 821 (1989).

McDaniel, Jay R., Note, Electronic Torts and Videotex-At the Junction of Commerce and Communication, 18 Rutgers Computer and Tech. L. J. 773 (1992).

McDaniel v. Coca-Cola Bottling, 2 S.E.2d 810 (1939).

McEwan. (1989). Dedicated computer crime units. Washington, DC: National Institute of Justice.

McGill University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

McGovern v. Van Riper, 54 A.2d 469 (1947).

Messick, David M., and Marilynn B. Brewer. (1983). Solving social dilemmas, in Review of Personality and Social Psychology (Vol. 4), edited by L. Wheeler and P. Shaver. Beverly Hills, CA: Sage, page 11-44.

Miami Herald Publishing v. Tornillo, 418 U.S. 241 (1974).

Michigan State University AUP [On-line]. Available as of July 1, 996: gopher:// gopher.eff.org/11/CAF/policies.

Midwest Video Corp. v. FCC, 571 F.2d 1025 (1978).

Miller, Philip H., Note, New Technology, Old Problem: Determining the First Amendment Status of Electronic Information Services, 61 Fordham L. Rev. 1147 (1993).

Milton, John. (1987). Paradise lost. New York: Chelsea House.

State of Minnesota v. Smith, 367 N.W.2d 497 (1985).

Moore, Barrington Jr. (1984). Privacy: Studies in social and cultural history. New York: Random House.

Mutual Film Corp. v. Industrial Comm'n, 236 U.S. 230 (1915).

Naughton, Edward J. Is Cyberspace a Public Forum? Computer Bulletin Boards, Free Speech, and State Action, 81 Geo. L. J. 409 (date).

Nebbia v. New York, 291 U.S. 502 (1934).

State of New Jersey v. Griffin, 202 A.2d 856, (1964).

New Mexico State University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

New Mexico Statutes §30-16A-1 (1992).

New York v. Belton, 453 U.S. 454 (1981).

Niblett, G.B.F. (1971). Digital information and the privacy problem. Baltimore, MD: Organization for Economic Co-operation and Development Informatics Studies.

Note, From Private Places to Personal Privacy: A Post-Katz Study of Fourth Amendment Protection, 43 N.Y.U. L. Rev. 968 (1968).

Note, The Message in the Medium: The First Amendment on the Information Superhighway, 107 Harv. L. Rev. 1061 (March 1994). Available as of July 1, 1996: http://www.swissnet.ai.mit.edu/6095/atricles/message-in-the-medium.txt.

Note, The Privacy Act of 1974: An Overview and Critique, 1976 Wash. U. L. Q. 667.

O'Brien, David M. (1979). Privacy, law, and public policy. New York: Praeger.

Ohio Revised Code §§2901.01 and 2913.01.

Ohio State University AUP [Online]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Oliver v. United States, 466 U.S. 170 (1984).

Olmstead v. United States, 277 U.S. 438 (1928).

Ostrom, Elinor. (1990). Governing the commons: The evolution of institutions for collective action. New York: Cambridge University Press.

Palko v. Connecticut, 302 U.S. 319 (1937).

Parker. (1989). Computer crime: Criminal justice resource manual. Washington, DC: National Institute of Justice.

Patterson, Frank Allen (Ed.). (1993). The student's Milton. New York: Columbia University.

Payton v. New York, 445 U.S. 573 (1980).

Pemberton v. Bethlehem Steel, 502 A.2d 1101 (1986).

Pennock, J. Roland, and John W. Chapman. (1971). Privacy. New York: Atherton Press.

People v. Cook, 22 Cal.3d 67 (date), 148 Cal.Rptr. 605, 538 P.2d 130.

People v. Heath, 72 Cal. Rptr 457 (1968), 458, 266 C.A.2nd 754.

People v. Manzi, 502 A.2d 1101 (1986).

People v. Perlos, 462 N.W.2d 310 (1990).

People v. Thomas, 169 Cal.Rptr. 570 (1980).

Perritt, Henry H. Jr., Dispute Resolution in Electronic Network Communities, 38 Vill. L. Rev. 349 (1993).

Perritt, Henry H. Jr., The Electronic Agency and the Traditional Paradigms of Administrative Law, 44 Admin. L. Rev. 79 (1992).

Perritt, Henry H. Jr., Tort Liability, the First Amendment, and Equal Access to Electronic Networks, 5 Harvard J.L. & Tech. 65 (1992).

Perritt, Henry H. Jr. (1992). Metaphors for understanding rights and responsibilities in network communities: Print shops, barons, sheriffs, and bureaucracies [On line]. Available as of July 1, 1996: http://finish.

Perritt, Henry H. Jr., Introduction: Symposium: The Congress, the Courts and Computer Based Communication Networks: Answering Questions About Access and Content Control, 38 Vill. L.Rev. 319 (1993).

Petrocelli, William. (1981). Low profile: How to avoid the privacy invaders. New York: McGraw-Hill Book Company.

Phillips v. Smalley Maintenance, 435 So.2d 705 (1983).

Pierson v. News Group Publications, 549 F.Supp 635 (1982).

Pool, Ithiel de Sola. (1983). Technologies of freedom. Cambridge, MA: Belknap Press.

Power, Kevin. (1994, April 10). Proposed wiretap law sets off debate over justice role. Government Computer News.

Prince v. St. Francis-St. George Hosp., 484 N.E.2d 265 (1985).

The Privacy Act of 1974, Pub. L. No. 93-579 (1974).

Privacy in the workplace: When employer-employee rights collide. (1978). New York: Alexander Hamilton Institute.

Prosser, Dean. Privacy, 48 Cal. L. Rev. 383 (1960).

Purdue University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Quarterman, John S. (1995, March 3). Internet communications services on NSFNET. Matrix News, 5(3) [On-line]. Available as of July 1, 1996: gopher://akasha.tic.com:70/matrix/news /v5/ports.501.

Rabel, Timothy R. (1992, March). Who's listening in on your portable phone? IEEE Software, 9(2), pp. 89-91.

Rakas v. Illinois, 439 U.S. 128 (1978).

Rand, Ayn. (1994). The fountainhead. New York: Plume.

Red Lion Broadcasting Co. v. FCC, 395 U.S. 367 (1969).

Regan, Priscilla M. (1995). Privacy, technology, and public policy. Chapel Hill, NC: University of North Carolina Press.

Reingold, Howard. (1996). The tragedy of the electronic commons [Online]. Available as of July 1,1996: http://www.well.com/user/hlr/tomorrow /tomorrowcommons.html.

Religious Technology Center v. Lerma, et. al., 95-1107-A E.D. Va. (November 29, 1995).

Restatement (second) of torts. (1979). St. Paul, MN: American Law Institute Publishers.

Riddle, Michael H. (1990). The electronic pamphlet: Computer bulletin boards and the law. Available as of July 1, 1996: http://www.swissnet.ai.mit.edu/finish.

Right to privacy in the age of telecommunication [On-line]. (1996, March 26). Available as of July 1, 1996: http://www.tscm.com/full-text.html.

Rivest, Ronald L. (1993, March). To tap or not to tap. Communications of the ACM, 36(3), page 39-40.

Roaden v. Kentucky, 413 U.S. 496 (1973).

Roberson v. Rochester Folding Box Co., 171 N.Y. 538 (1902).

Roe v. Wade, 410 U.S. 113 (1972).

Rogers v. Grimaldi, 875 F.2d 994 (1989), 16 Media L. Rev. 1648.

Rosenberg v. United States, 346 U.S. 273 (1953).

Rosenberg v. United States, 346 U.S. 273 (1953).

Rotenberg, Marc. (1993, August). Communications privacy: Implications for network design. Communications of the ACM, 36(8), pp. 61-68.

Rothfeder, Jeffrey. (1992). Privacy for sale: How computerization has made everyone's private life an open secret. New York: Simon & Schuster.

Rousseau, Jean. (1978). The social contract. New York: St. Martins Press.

Roviaro v. United States, 353 U.S. 53 (1957).

Rubin, David. (1984). The rights of teachers: The basic ACLU guide to teacher's constitutional rights. New York: Bantam Books.

Rubin, Michael Rogers. (1988). Private rights, public wrongs: The computer and personal privacy. Norwood, MA: Alex Publishing Corporation.

Ryder, Martin and Brent Wilson. (1996). From local to virtual learning environments: Making the connection [On-line]. Available as of November 1, 1996: http://www.cudenver.edu/~mryder/aera95.html

Sable Communications v. The FCC, 492 U. S. 115, 124 (1989).

Samar, Vincent. (1993). The right to privacy: Gays, lesbians, and the constitution. Philadelphia, PA: Temple University Press.

Sassan, Anthony J., Note, Cubby, Inc. v. CompuServe, Inc.: Comparing Apples to Oranges: The Need for a New Media Classification, 5 Software L. J. 821 (1992).

Schlachter, Eric. Essay, Cyberspace, the Free Market, and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions, 16 Hastings Comm/Ent L. J. 87 (1993).

Schiller, Herbert. (1994, March). Information superhighway: Paving over the public, Z Magazine.

Schoeman, David. (1992). Privacy and social freedom. Cambridge, MA: MIT Press.

Seipp, English Judicial Recognition of a Right to Privacy, 3 Oxford J. Leg. Stud. 325 (1983).

Sergent, Randolph S., Note: A Fourth Amendment Model for Computer Networks and Data Privacy, 81Va. L. Rev. 1181 (May, 1995).

Shaprio, Fred R. (1987). The most cited law review articles. Buffalo, NY: W. Hein Co.

Sieghart, Paul. (1976). Privacy and computers. Great Britain: The Hollen Street Press Ltd.

Silverglate, Harvey A. (1994, December 24). Statement of Silverglate and Good concerning the dismissal of the indictment in United States v. David M. LaMacchia. Available as of July 1, 1996: http://www.swissnet.ai.mit.edu /6095/articles/dml/lamacchia.html.

Silverglate, Harvey A., Computer Crime in Massachusetts, 38 Boston Bar J. 5 (Mar-Apr 1994).

Silverglate, Harvey A. and Thomas C. Viles. (1991, May). Constitutional, legal, and ethical considerations for dealing with electronic files in the age of cyberspace. Paper presented at the 1991 Federal Enforcement Conference, Georgetown University Law Center, Washington, DC.

Silverman v. United States, 365 U.S. 505 (1961).

Smith, Robert Ellis. Quoted in Andre Bacard. (1995). The computer privacy handbook. Berkeley, CA: Peachpit Press. page 17.

Smith, H. Jeff. (1994). Managing privacy: Information technology and corporate America. Chapel Hill, NC: The University of North Carolina Press.

Smith v. California, 361 U.S. 147 (1959).

Smith v. Maryland, 442 U.S. 735 (1979).

Soma, John T. et al., Legal Analysis of Electronic Bulletin Board Activities, 7 W. New Eng. L. Rev. 571 (1985).

Stanford v. State of Texas, 379 U.S. 476 (1965), reh den, 380 U.S. 926 (1965).

Steele v. Offshore Shipbuilding, 867 F.2d 1311 (1989), reh den 874 F.2d 821 (1989).

Stein, Arnold. (1952). Answerable style: Essays on paradise lost. Minneapolis, MN: University of Minnesota Press.

Sterling, Bruce. (1995). The hacker crackdown. New York: Bantam Books.

Steve Jackson Games v. United States Secret Service, 36 F.3d 457 (1994); 1994 U.S. App. LEXIS 30323.

Stevens, George E. and Harold M. Hoffman., Tort Liability for Defamation by Computer, 6 Rutgers J. Computers & L. 91 (1977).

Stikes v. Chevron USA, 914 F.2d 1265 (1990).

Story, William W. (1847). A treatise on the law of contracts (2nd ed.). City: Publisher.

Stratton Oakmont v. Prodigy, 1995 NY Misc. LEXIS 229.

Struner v. Dispatch Printing, 442 N.E.2d 129 (1982).

Stuntz, William J., Warrants and Fourth Amendment Remedies, 77 Va. L. Rev. 881 (1991).

Sun v. Langston, 316 S.E.2d 172 (1984).

Taviss, Michael L., Comment, Dueling Forums: The Public Forum Doctrine's Failure to Protect the Electronic Forum, 60 U. Cin. L. Rev. 757 (1992).

Telecommunications Act of 1996, 47 U.S.C §151 (1996).

Telecommunications Research & Action Center v. FCC, 801 F.2d 501 (1986).

Terry v. Ohio, 392 U.S. 1 (1968).

Thompson, Judith J. (1995, Summer). The right to privacy. Philosophy and Public Affairs, 4(4).

Thornburgh v. American College of Obstetricians & Gynecologists, 476 U.S. 747 (1986).

Tribe, Laurence H. (1988). American constitutional law (2d ed.). Mineola, NY: Foundation Press.

Tribe, Laurence H. (1991, March). The Constitution in cyberspace: Law and liberty beyond the electronic frontier. Keynote address at the First Conference on Computers, Freedom and Privacy, Boston, MA. Available as of July 1, 1996: http://www.swissnet.ai.mit.edu/6095/articles/tribe-constitution.txt.

Trubow, George B. (1992, March). When is monitoring e-mail really snooping? IEEE Software, 9(2), page 97.

Tuerkheimer, Frank M. (1993, August). The underpinnings of privacy protection. Communications of the ACM, 36(8).

Turner, Roy M. (1991, January). The tragedy of the commons and distributed AI systems [Online]. Paper presented at the 12th International Workshop on Distributed Artificial Intelligence, University of New Hampshire, Durham, NH. Available as of July 1, 1996: http://cdps.umcs.maine.edu/Papers/1993/TofCommons/TR.html.

Tye, Larry. (1993, September 5). Privacy lost in high-tech era. Boston Sunday Globe, page 18.

Umar, Amjad. (1993). Distributed computing. Englewood Cliffs, NJ: Prentice Hall.

U.S. Congress, Office of Technology Assessment. (1986). Federal government information technology: Electronic record systems and individual privacy. (Office of Technology Publication No. OTA-CIT-296). Washington, DC: U.S. Government Printing Office.

U.S. Department of Health and Human Services and U.S. Department of Education, (1993). Together we can: A guide for crafting a profamily system of education and human services. Washington, DC: U.S. Government Printing Office.

U.S. Privacy Protection Study Commission. (1977, July). Personal privacy in an information society (U.S. Privacy Protection Study Commission ISBN/ISSN 8460966 10373764). Washington, DC: Author.

United States v. Bell, 335 F.Supp. 797 (1971), aff'd (CA2 NY) 464 F.2d 667, cert. den. 409 U.S. 991 (1972), 34 L.Ed.2d 258, 93 S.Ct. 335.

United States v. Choate, 576 F.2d 165 (1978), cert. denied, 439 U.S. 953 (1978).

United States v. David, 756 F.Supp. 1385 (1991).

United States v. David M. LaMacchia, Criminal No. 94-10092RGS (March 1994). Available as of July 1, 1996: http://www.swissnet.ai.mit.edu/6095 /articles/dml/lamacchia.html. (LaMacchia, an electrical engineering and computer science student, used two MIT computers to create bulletin boards from which Internet users could post or copy commercial copyrighted software worth close to $1 million.)

United States v. Hagarty, 388 F.2d 713 (1968).

United States v. Jacobsen, 466 U.S. 109 (1984).

United States v. Karo, 468 U.S. 705 (1984).

United States v. Lefkowitz, 285 U.S. 452 (1932).

United States v. Miller, 425 U.S. 435 (1976).

United States v. Moreno 475 F.2d 44 (1973), cert. den. 414 U.S. 840 (1973).

United States v. Nasser, 476 F.2d 1111 (1973).

United States v. Paramount Pictures, Inc., 334 U.S. 131 (1948).

United States v. Place, 462 U.S. 696 (1983).

United States v. Powell, 929 F.2d 1190 (1991).

United States v. Smith, 978 F.2d 171 (1992).

United States v. Turk, 526 F.2d 654 (1976), cert. denied, 429 U.S. 823 (1976).

United States v. White, 401 U.S. 745 (1971).

United States v. Willis, 759 F.2d 1486 (1985), cert. denied, 474 U.S. 849 (1985).

University of California at Berkeley AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

University of Hawaii at Manoa AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

University of Illinois at Chicago AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

University of Illinois-Urbana Champagne AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

University of Massachusetts at Amherst AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

University of Michigan AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

University of New Mexico AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

University of Pittsburgh AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

University of Texas AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

University of Wisconsin at Milwaukee AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

Update on New York State Bill. (1996, February 18). BillWatch. Available as of July 1, 1996: http://www.vtw.org/billwatch.

Vassiliades v. Garfinckel, Brooks Bros., 492 A.2d 580 (1985).

Walker v. City of Hutchinson, 352 U.S. 112 (1956).

Walter v. United States, 447 U.S. 649 (1980).

Ware, Willis H. (1985, August 13). Emerging privacy issues. Paper presented at the 1985 IFIP/SEC Conference at Trinity College, Dublin, Ireland.

Warren, Samuel and Louis Brandeis, The Right to Privacy, 4 Harvard L.Rev. 193 (1890).

Washington Univ. AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org /11/CAF

Wayner, Peter. (1993, May). Should encryption be regulated? Byte, 18(6), page 129.

Westin, Alan. (1967). Privacy and freedom. New York: Anthenum Press.

Whalen v. Roe, 429 U.S. 589 (1976).

White, James B. (1985). The legal imagination. Chicago: University of Chicago Press.

Whitney v. California, 274 U.S. 357 (1927).

Wildstrom, Stephen H. (1993, October 4). Spy v. computer nerd: The fight over data security. Business Week, page 43.

Williams, Raymond. (1976). Keywords: A vocabulary of culture and society. London: Fontana Press.

Willner v. Committee on Character and Fitness, 373 U.S. 96 (1963).

Yin, Tung, Comment, Post-Modern Printing Presses: Extending Freedom of Press to Protect Information Services, 8 High Tech. L. J. 311 (1993).

Young, John B. (1978). Privacy. New York: John Wiley & Sons.

Acceptable Use Policies

AUP-Working Group of Internet Engineering Task Force. (1995, July). Acceptable use policy definition [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Boston University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

University of California at Berkeley AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

Computer and Academic Statement from the Electronic Frontier Foundation AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11 /CAF/policies.

Dalhousie University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Electronic Freedom Foundation AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

University of Hawaii at Manoa AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

University of Illinois at Chicago AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

University of Illinois-Urbana Champagne AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

Iowa State University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Kansas State University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

James Madison University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Mankato State University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

McGill University AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

University of Massachusetts at Amherst AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

University of Michigan AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

Michigan State University AUP [On-line]. Available as of July 1, 996: gopher://gopher.eff.org/11/CAF/policies.

University of New Mexico AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

New Mexico State University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Ohio State University AUP [Online]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

University of Pittsburgh AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

Purdue University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

University of Texas AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.

University of Wisconsin at Milwaukee AUP [On-line]. Available as of July 1, 1996: gopher://gopher.eff.org/11/CAF/policies.

Washington University AUP [On-line]. Available as of July 1, 1996: gopher:// gopher.eff.org/11/CAF/policies.